Secure Schools

Building cyber resilience in education

Stage 1

Audit Report

Date: 18/04/2022
Lead Assessor: Paul Alberry
SENSITIVE

Chelmsford County High School for Girls

Contents

Executive Summary 4
Audit in Numbers 4
Culture vs Written Policy 4
IT Department Participation 4
Training and Awareness 5
Password Security and Multi-Factor Authentication 5
Risk Management 5
Testing and Measuring Progress and Conformance 5
How To Use This Report 6
Action Plan vs Auditor's Comments 6
Action Plan 7
Prioritisation Matrix 7
Recommended Action Points 8
Further Suggestions 15
Cyber Essentials Preparation Action Plan 16
Scope 19
Framework 19
Department for Education (DfE) 19
Education and Skills Funding Agency (ESFA) 19
National Cyber Security Centre (NCSC) 19
IASME Consortium 20
Sources of Information 20
Assessment Team 21
Gap Analysis 22
Self-Evaluation Assessment 22

Stage 1 Audit Report

Chelmsford County High School for Girls

Title	Chelmsford County High School for Girls Cyber Security Audit Report 2022			
Created By	Paul Alberry of Secure Schools Ltd			
Date Created	15/03/2022			
Maintained By	Paul Alberry of Secure Schools Ltd			
Version Number	**Modified By**	**Modifications Made**	**Date Modified**	**Status**
1.0	TATENDA MUNAKI	PRODUCED GAP ANALYSIS	15/03/2022	DRAFT
1.1	PAUL ALBERRY	ADDED CES FIELDS TO ACTION PLAN AND ADJUSTED FORMATTING	07/04/2022	DRAFT
1.2	JOSEPHINE TURNER	PROOF READING	12/04/2022	DRAFT
1.3	PAUL ALBERRY	PUBLISHED FIRST DRAFT	18/04/2022	DRAFT

Chelmsford County High School for Girls

Executive Summary

Audit in Numbers

Between March and April 2022, Secure Schools conducted a cyber security audit at Chelmsford County High School for Girls. This audit evaluated the school's compliance with the current expectations from the DfE and ESFA, combined with the IASME Governance standard for information security governance which includes the Cyber Essentials scheme.

The self-evaluation phase of the review identified **38** areas of non-compliance against the standards identified on pages 19-20, the majority of which the school has made good progress with but requires some development to meet the above standards.

In number of non-compliance areas, this review places the school 'above average' in comparison to similar audits Secure Schools has performed within this academic year. Although this report will refer to negative findings as 'non-compliances and non-conformances', it should be noted that unless stipulated specifically, such findings are not statutory or regulatory requirements of the school.

Throughout the knowledge transfer conversations - which are carried out to triangulate and validate the self-evaluation phase – we identified some areas in which the school is exceeding its self-evaluation. In such cases, we have excluded related action points from the action plan. In addition, these areas of non-compliance and part-compliance are closely linked, and most can be resolved by a handful of action points. We have created a suggested action plan (p7-18) which details our recommended action points (p8-18) and plotted these action points on a prioritisation matrix according to their impact and difficulty to implement.

Culture vs Written Policy

The school has a good culture for managing information technology and it became clear throughout the audit that the development of this culture is driven by strong leadership. However, some elements of the school's information management policies exist only in culture and are not underpinned by formal, written documentation. This presents a risk that a change in staff that drive this culture will likely affect the security of information systems. It is also difficult for the school to evidence compliance without written records. Recommendations as to which areas of the management system should be developed are included in the action plan.

IT Department Participation

Chelmsford County High School for Girls' IT department was very supportive throughout the process. The department was well represented, with the school's IT Manager present throughout the entire discussion.

Training and Awareness

The school does not currently have a formal staff cyber security awareness training programme. It should consider prioritising deploying a cyber security awareness training programme as advised from the Department for Education in its October 2020 update to school leaders. When looking for a solution, the school should ensure that the training package includes *at least: password security training (aligned to the school's password policy) and phishing threat awareness training*. It is important that not only is training prescribed and completed by all staff, but very specific, low-level coaching is provided periodically that demonstrates how the high-level techniques covered in the training are applied in a school's daily working context. For example: *How do we generate, save, and retrieve passwords at Chelmsford County High School for Girls? How do we report an incident at Chelmsford County High School for Girls? How do we use Chelmsford County High School for Girls' email security features to recognise phishing attempts?*

Password Security and Multi-Factor Authentication

Password security is a challenging area for most organisations, including educational establishments. Upon speaking to staff at the school, we identified that it is highly likely that staff are using the same password across several of their 'work' accounts, and perhaps even using the same password as they use for some of their 'personal' or 'home' accounts such as social networks. The more often a password is used across different devices and services, the more likely that the password will be compromised. With compromised passwords associated to staff names and email addresses, the risk of school accounts being breached increases. To reduce this risk, staff could use 'password managers' to store strong, unique passwords for every account and ensure that no personal passwords are re-used for work accounts. Implementing a password manager means that staff never have to remember their passwords and should make working with IT easier.

Risk Management

The school does include the risk area of cyber security within its existing risk management system. Although reviewing the risk register is beyond the scope of this assessment, we feel that the school demonstrated a very good understanding of how cyber security risk fits into the school's wider risk management programme.

Testing and Measuring Progress and Conformance

Once the school has made progress with cyber security policy – with the proposed developments according to this review's action plan - the school should begin to expand its programme for testing 'reality' against policy for staff behaviour and systems configuration.

Further assurance can be achieved by conducting internal vulnerability assessments and penetration testing using tools and techniques leveraged by cybercriminals in a safe and controlled environment. Using policy to create targets and key performance indicators, and subsequently testing performance, can be an effective way of maintaining continuous improvement. Building upon the progress made following this review with technical testing will also provide additional assurance to the school's stakeholders, proving that the intentions set by policy are maintained in practice.

During the knowledge transfer conversations, the school acknowledged that many of its students are talented and highly capable with technology. It should consider integrating the testing popular 'hacking' hardware and software tools into its assurance programme to ensure that controls are in-place for tools that could be used by students (for example, the locking of communications equipment cabinets around the school).

How To Use This Report

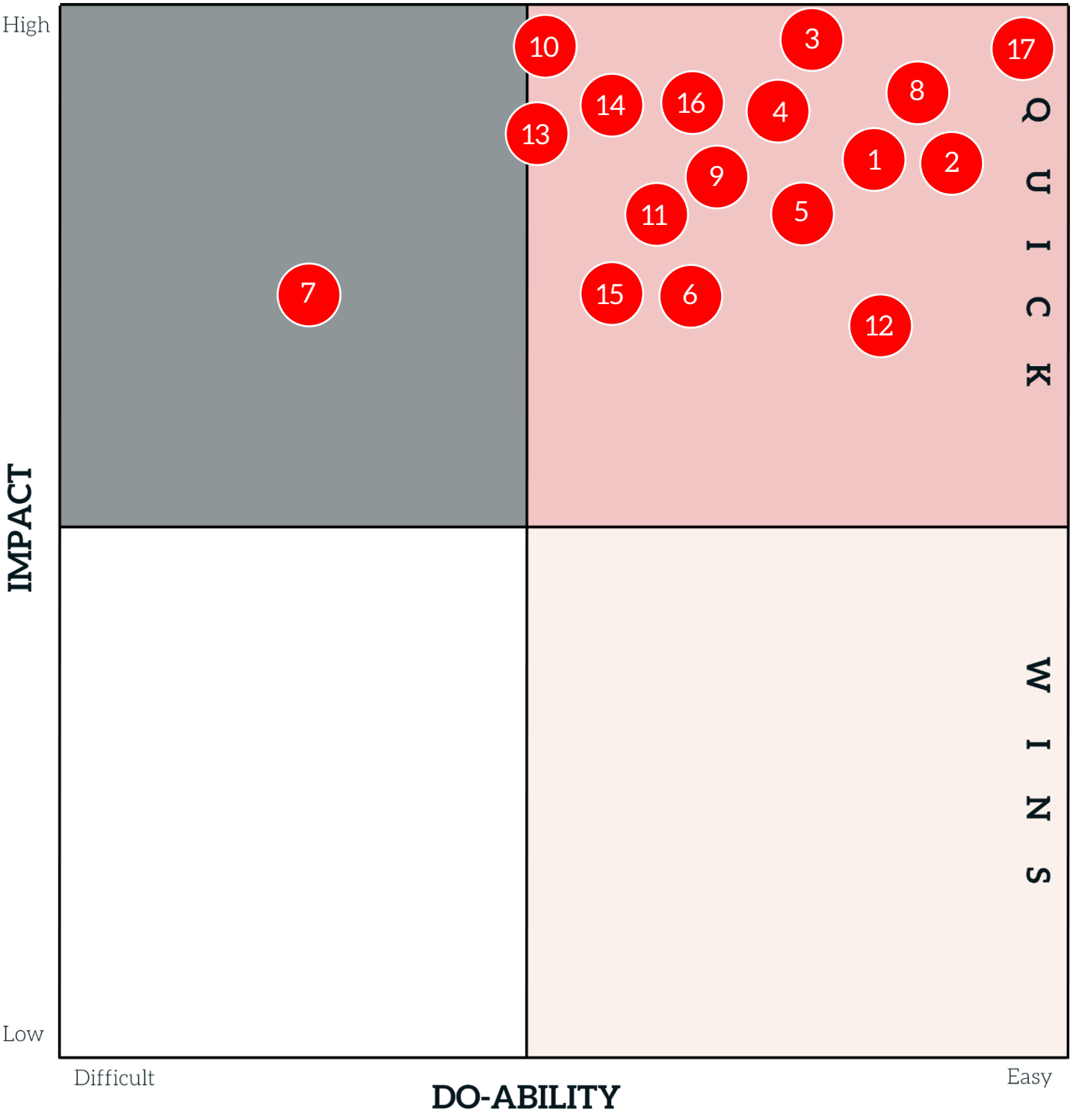
Action Plan vs Auditor's Comments
This report contains a combination of 'action points' and 'auditor comments'. *Action Points* are actions that we recommend the school considers based upon the findings of the audit. They may be critical elements identified during the assessment of the 'self-evaluation form' or issues raised during conversations with the organisation's staff. Only *Action Points* are listed in the Action Plan (p8-18).

Other findings, which we have assessed to be as less critical are listed in the final column of the Gap Analysis table (p22-end). We recommend that the school reviews each auditor comment in addition to the Action Plan, so that the school can make its own assessment. On most occasions, this decision should be made with the IT department. Please feel free to contact Secure Schools for any support with making individual decisions as to whether to implement the advice provided in auditor comments.

Chelmsford County High School for Girls

Action Plan

Prioritisation Matrix



Chelmsford County High School for Girls

Recommended Action Points

Action Point	Relating Standard/Guidance	Assigned to (Person or Department)	Priority (Low/Medium/High)	Progress (Percent)	Due Date	Decided Action
1. Implement cyber security standing agenda items for the Finance and Premises Committee (or the Executive Committee). The NCSC Questions for Governors and Trustees could be used to form the agenda.	IASME GOVERNANCE	----------	High	_____%	----------	
2. Formally appoint a board member responsible for cyber security.	IASME GOVERNANCE	----------	High	_____%	----------	

3. Document in formal written policies how the school approaches cyber security. We recommend this is achieved by breaking up the school's existing Cyber Security Policy into the following policies: - Internal Information Security Policy (for all staff) - IT acceptable use - Social engineering - Passwords and authentication - Use of encryption - Internal Information Security Policy (for IT staff and school leadership) - Password policy - Firewalling policy - Access control policy - Secure configuration policy - Anti-malware policy - Patch management policy - Asset management policy - Removable media policy - Domain security policy - Supply chain security policy - IT asset disposal policy Ensure that the school senior leaders, business leaders, and governors support these policies.	IASME GOVERNANCE CYBER ESSENTIALS	_____	High	_____%	_____	

Chelmsford County High School for Girls

4. Implement a formal staff and board member cyber security awareness training programme that includes specific guidance for creating (and managing) passwords and recognise the characteristics of phishing emails, that also allows for monitoring and recording performance. Report to the board at least annually.	IASME GOVERNANCE + DfE Guidance (notification to school leaders October 2020) NCSC Advice	----------	High	_____%	----------	
5. Formalise a review process to be followed before implementing significant changes to IT systems, software applications or networks. This should be authorised by the board.	IASME GOVERNANCE	----------	Medium	_____%	----------	
6. Establish a formal written cyber security incident management plan which includes: - Definition of an incident - How to preserve evidence - Notification of bodies - Roles and responsibilities - Documented lessons learned	IASME GOVERNANCE + DfE Guidance (notification to school leaders October 2020) NCSC Advice	----------	Medium	_____%	----------	

Chelmsford County High School for Girls

7. Run through the formal written cyber security incident management plan as a tabletop exercise.	IASME GOVERNANCE + DfE Guidance (notification to school leaders October 2020) NCSC Advice	_____	Medium	_____%	_____	
8. Ensure the board allocates and monitors sufficient resources to support cyber security initiatives.	IASME GOVERNANCE + DfE Guidance (notification to school leaders October 2020) NCSC Advice	_____	Medium	_____%	_____	
9. Add findings and actions of this report to a 'Cyber security' section in the school's risk register.	IASME GOVERNANCE	_____	Medium	_____%	_____	

Chelmsford County High School for Girls

10. Periodically scan IT systems for known vulnerabilities so that security risks can be treated before being exploited. Report to the board at least annually.	IASME GOVERNANCE	_____	Medium	_____%	_____	
11. Periodically perform penetration tests to measure the effectiveness of already implemented administrative and technical/logic controls. Report to the board at least annually.	IASME GOVERNANCE	_____	Medium	_____%	_____	
12. Test the school's IT network's ability withstand the use of popular 'hacking' tools (hardware and software), that could be used by students.		_____	Low	_____%	_____	

Chelmsford County High School for Girls

13. Remove software that is no longer supported to receive security updates from laptops, computers, servers, tablets and smartphones.	IASME GOVERNANCE CYBER ESSENTIALS	_____	High	_____%	_____	
14. Maintain a 'Special Privileges Register' that records users with higher level privileges, the justification for high privileges and should be reviewed at least annually.	IASME GOVERNANCE CYBER ESSENTIALS	_____	High	_____%	_____	

Chelmsford County High School for Girls

15. Implement a monitoring system to alert administrators of suspected ransomware attacks in motion.	IASME GOVERNANCE	_____	Medium	_____%	_____	
16. Enable staff to use strong, unique passwords for accessing devices, software and cloud services by providing access to a password manager solution. Enforce this practice by policy and enable with training. *The school could use the built-in password management features in web browsers as a low-cost alternative to a commercial password manager.*	IASME GOVERNANCE CYBER ESSENTIALS	_____	High	_____%	_____	
17. Schedule annual surveillance audits that support this action plan.		_____	Medium	_____%	_____	

Chelmsford County High School for Girls

Further Suggestions

S1. Consider registering the school with the NCSC's Early Warning service (available free of charge to all UK organisations).	National Cyber Security Centre	----------	Medium	_____%	----------	
S2. Consider registering the school with the NCSC's Web Check and Mail Check services (made available free of charge to UK schools in April 2022).	National Cyber Security Centre	----------	Medium	_____%	----------	
S3. Consider implementing Logging Made Easy (LME) to manage security events across the Windows devices in the schools' IT estate.	National Cyber Security Centre	----------	Medium	_____%	----------	

Chelmsford County High School for Girls

Cyber Essentials Preparation Action Plan

Admin steps to prepare for Cyber Essentials						
A. Set a date to aim for Cyber Essentials certification. Ensure that the date doesn't coincide with any upcoming changes to the Cyber Essentials scheme requirements.	CYBER ESSENTIALS	-		_____%	_____	
B. Work with a Cyber Essentials Certification Body to determine a scope for Cyber Essentials certification.	CYBER ESSENTIALS	-		_____%	_____	

Chelmsford County High School for Girls

C. Prepare a spreadsheet document containing all of the school's IT devices. Include: - *Device type* - *Device manufacturer* - *Device model* - *Operating System* - *Operating System version and build* - *Scheduled retirement date*	CYBER ESSENTIALS	-		_____%	_____	
Note: The school could consider keeping and maintaining this document to perform risk assessments on devices, or groups of devices based upon their applicable threats.						

Chelmsford County High School for Girls

D. Prepare a spreadsheet document containing all of the software installed on the school's IT devices. Include: - *Vendor/developer name* - *Software name* - *Software version number* - *Release date* - *Supported to receive security updates?*	CYBER ESSENTIALS	-		_____%	_____	
Note: The school could consider keeping and maintaining this list document to perform risk assessments on software and services based upon their applicable threats.						

Chelmsford County High School for Girls

Scope

We have conducted this audit assignment according to the approved audit plan (Stage 1 Pre-Audit Pack). The time period covered by the audit is from March to April 2022. The logical scope of this audit is the school in its entirety and includes the following areas of information security governance:

1. Understanding your school or trust
2. Leadership, risk management and governance
3. Information assets and risk management
4. Managing cloud services
5. *Data protection: data security – not included*
6. People
7. Cyber security policy
8. Change management
9. Security testing, audit and assurance
10. Incident management, continuity and recovery

Framework

Secure Schools has determined a standard that represents an appropriate level of cyber security for UK schools and Trusts while including expectations set by UK government agencies. Listed below are the sources and schemes combined to determine the standard for the Secure Schools Stage 1 Pre-Audit.

Department for Education (DfE)
The DfE currently communicates expectations to school leaders by directly addressed letters. These letters usually highlight current prevalent risks that are identified by its partner government organisation, the National Cyber Security Centre.

Education and Skills Funding Agency (ESFA)
The ESFA is a key stakeholder for local authorities, academies and academy Trusts. As a government department that provides funding and flow of potentially sensitive information, it sets cyber security conditions in its contracts for funding in addition to requiring the subject to be included by audit and risk committees.

National Cyber Security Centre (NCSC)
The NCSC is an organisation of the UK Government that provides advice and support for the public and private sector in how to avoid computer security threats. It developed the Cyber Essentials certification scheme, which helps organisations guard against common cyber threats and demonstrate commitment to cyber security.

Chelmsford County High School for Girls

IASME Consortium
The IASME Consortium is the NCSC's Cyber Essentials Partner. In addition to delivering the Cyber Essentials scheme, they also developed the IASME Governance standard during a government funded project to create a cyber security standard which would be an affordable and achievable alternative to the international standard, ISO 27001. The IASME Governance standards allows organisations to demonstrate their level of cyber security for a realistic cost and indicates that they are taking good steps to properly protect information.

Sources of Information

Chelmsford County High School for Girls completed the Secure Schools Stage 1 Pre-Audit Self-Evaluation Form, which provided most of the information that contributed to this audit. The answers to this Self-Evaluation Form enabled our team to gauge the school's understanding and compliance with the four framework areas. Our lead assessor used professional judgement to determine the areas that required further explanation or evidence of compliance.

Discussions were held by phone call or video teleconferencing with the personnel in the following roles:

- School Business Manager
- School IT Manager
- Assistant Head Teacher
- Admin Staff Member

Any appointments that were scheduled but not listed above were uncontactable during the review.

Although the methodology used for this audit provides a balanced approach, there are inherent limitations:

- There is a possibility of human error due to carelessness, distraction, mistake of judgement or lack of understanding in the subject area.
- There is a possibility that a source of information abused their responsibility in this information and provided purposefully inaccurate information.

Chelmsford County High School for Girls

Assessment Team

Paul Alberry was the lead assessor in this audit.

Tatenda Munaki was the assessor for the completed Self-Evaluation Form.

Paul Alberry and Paul Armstrong conducted discussions with personnel at the school.

Chelmsford County High School for Girls

Gap Analysis

Self-Evaluation Assessment

Question	Answer	Assessment	Assessor's Comments	Auditor's Comments
Section 1 - Understanding Your School or Trust				
1.1 What does this audit cover?	A single school or academy	**Compliant**		
1.2 Please list the geographical location (full address) of your school(s).	Chelmsford County High School for Girls Broomfield Road Chelmsford Essex CM1 1RW	**Compliant**		
1.3 Please list the number of employees in each school.	131	**Compliant**		
1.4 Please state the total number of employees that are considered as remote or home workers. *A remote or homeworker can be any employee who is required to work from home for any amount of time.*	0	**Compliant**		
1.5 What is the full name and job title of the person responsible for the overview of this internal audit?	Melissa Mulgrew - Business Manager	**Compliant**		

Chelmsford County High School for Girls

1.6 Does this person have overall responsibility for cyber security of your school?	Yes	Compliant	
- If no, who it this in your school?			
1.7 Has the person with overall responsibility for cyber security received specific training to carry out this role?	No	Non-compliant	The school should consider ensuring that the person responsible for cyber security receives adequate training to effectively carry out the duties associated with this role.
1.8 Is this person also responsible for ensuring that all other staff receive appropriate cyber security awareness training?	Yes	Compliant	
- If no, who it this in your school?			

Chelmsford County High School for Girls

1.9 What is the name and job title of the person in your school responsible for making IT decisions?	Melissa Mulgrew / Tony Cable -Business Manager / IT Manager	**Compliant**	[redacted]
1.10 Does your school accept credit card payments?	Yes	**Compliant**	
- If yes, does your school store this credit card information?	No	**Compliant**	
- If yes, are all the systems used to process this information compliant to the PCI-DSS regulation?	[redacted]		

Chelmsford County High School for Girls

Section 2 - Cyber Security Leadership & Governance			
2.1 Is there a governance committee structure for managing information risk as part of school risk management?	Yes	**Compliant**	
2.2 Does your board have a named member responsible for cyber security?	No	**Non-compliant**	The board should have a named member responsible for cyber security. Improving cyber resilience normally requires changes to policies and procedures that might require board-level approval and support.
- If yes, please provide the name of this person.			
2.3 Is cyber security a standard agenda item on the audit and risk committee?	No	**Non-compliant**	Cyber security should be a standard agenda item on the audit and risk committee.
2.4 Does your school have a policy - suite of policies - that refer to cyber security which has/have been ratified by the board and signed by the board member responsible for cyber security?	No	**Non-compliant**	It is very important to document in formal written policies how the school approaches cyber security. These policies should be renewed at least annually.

Chelmsford County High School for Girls

- If yes, are the policies always reviewed at least annually?	[redacted]			
2.5 Are changes to your school's computers, networks and software applications controlled using documented procedures that the board has authorised?	No	Non-compliant	[redacted]	The school should consider formalising a clear change management process used to approve and track all significant changes to the school's computers, networks and software applications.
2.6 Is the board aware of when your school had its last vulnerability scan and how regularly they take place?	No	Non-compliant	[redacted]	Vulnerability scans expose cyber security risks. Providing vulnerability scan reports to the board can be a good way to provide assurance that policies are being followed. The school should consider requiring regular vulnerability scan reports to be presented to the board by policy.
2.7 Is the board aware of when the last penetration test was carried out in your school and how regularly they take place?	No	Non-compliant	[redacted]	Penetration tests can expose cyber security risks not identified using vulnerability scans as well as validate risks that have already been identified. Providing penetration test reports to the board can be a good way to provide assurance that

Chelmsford County High School for Girls

				policies are being followed. The school should consider commissioning penetration tests that measure the school's resilience to cyber-attacks that are taking place on educational establishments.
- If yes, please provide an example of how you acted on the outcome to improve security.				
2.8 Is regular, accurate and up-to-date information provided to the board to support their monitoring role in assessing the effectiveness of your school's cyber security risk management?	No	**Non-compliant**		The school should consider requiring regular cyber resilience reports to be presented to the board on a regular basis that include; vulnerability management, risk management and staff awareness training performance.
2.9 Is a periodic cyber security summary report disseminated at least annually with the whole board?	No	**Non-compliant**		At a minimum, the whole board should receive a report every year detailing school cyber resilience, including staff awareness training, number of incidents reported, risks mitigated and untreated risks.

Chelmsford County High School for Girls

2.10 Does the board allocate and monitor specific spending to address cyber resilience?	No	**Non-compliant**	[redacted]	Allocating and monitoring the allocation of resources to improve cyber resilience could help with cyber security action plan progress.
2.11 Does your school have an insurance policy in place that covers cyber security related incidents?	Yes	**Compliant**		
2.12 Does your school train staff and board members on the common cyber security threats and incidents that schools experience?	No	**Non-compliant**		The school should consider implementing a formal staff and board member cyber security awareness programme that allows for monitoring and recording performance.
2.13 Does the school's risk register contain a cyber security section, which includes IT and data risks?	Yes	**Compliant**		

Chelmsford County High School for Girls

- If yes, does this get formally reviewed at least once a year and approved at board level?	Yes	**Compliant**	
2.14 Are identified cyber security risks always marked as acceptable or unacceptable?	Question not answered	**Non-compliant**	Action points from this review could be included and individually assessed as cyber security risks.
- If yes, are unacceptable cyber security risks always followed up with an action plan?			
- If yes, do these action plans get reviewed at least termly at the audit and risk meetings and the risk register amended when appropriate?			
2.15 Is the school prepared for a cyber security critical incident?	Question not answered	**Non-compliant**	The DfE are advising schools to develop - and prepare to enact - a cybersecurity incident management plan. This plan should include the definition of an incident, how to preserve evidence, notification of bodies, roles and responsibilities and documented lessons learned. Testing this

Chelmsford County High School for Girls

				plan is a good way to demonstrate readiness.
- If yes, has the school prepared a formal cyber security incident management plan?	[redacted]			
- If yes, does the cyber security incident management plan include notification of all the required agencies; local law enforcement, National Cyber Security Centre, ActionFraud and Department for Education?				
- If yes, is the cyber security incident management plan tested annually?				

Chelmsford County High School for Girls

- If yes, is the plan reviewed considering the response?	[redacted]			
2.16 Does the school have a process for reviewing cyber security policies that includes consultation with a subject expert?	No	**Non-compliant**	Policies need to be reviewed regularly to ensure they are aligned to and support the latest technology, standards, and regulations.	The school should consider consulting with a subject matter expert when implementing and reviewing cyber security specific policy.
2.17 Do the school's policies detail how it will deal with incidents that threaten its viability by invoking business continuity measures?	Yes	**Compliant**	[redacted]	
2.18 Do the school's policies refer to home and mobile working?	Yes	**Compliant**		

Chelmsford County High School for Girls

2.19 Do the school's policies refer to computer and network security?	Yes	**Compliant**		
2.20 Do the school's policies refer to personnel security? (For example; identity checking, vetting and stranger challenging).	Question not answered	**Non-compliant**	Staff and contractor identity verification, vetting and stranger challenging should be covered by the trust's policies.	The school should consider formalising a written policy that details how it manages personnel security.
2.21 Do the school's policies refer to physical and environmental security?	Yes	**Compliant**		
If yes...				

Chelmsford County High School for Girls

- Does the building have effective physical protection and, if indicated by a risk assessment, surveillance and monitoring?	Yes	**Compliant**	
- Are only authorised personnel who have a justified and approved business case given access to restricted areas containing information systems or stored data?	Yes	**Compliant**	
- If yes, please explain how this is achieved.	Physical - no restrictions in place Network - access controls in place	**Non-compliant**	The school should formalise in written policies how it ensures that adequate physical controls are implemented e.g. locks, biometric systems, alarms etc., to restrict access to authorised personnel only.
- Are devices which require particular operating conditions (such as heating and cooling) always provided with a suitable environment within the guidelines set out by their respective manufacturers?	Yes	**Compliant**	

Chelmsford County High School for Girls

- If yes, please explain how this is achieved.	Aircon in IT suites & server rooms	**Compliant**
2.22 Does your school policy permit all staff to use removable media, such as USB storage?	No	**Compliant**
If yes…		
- Please explain how this is secured.		

Chelmsford County High School for Girls

- Is a dedicated machine used to scan removable media for viruses and malware?	[redacted]		
2.23 Do the school's policies refer to information asset management, including removable media?	Yes	Compliant	
2.24 Does the school have a policy that details acceptable IT use?	Yes	Compliant	
2.25 Does the school have a policy that details how it manages authentication and access to information?	No	Non-compliant	The school should consider formalising a written policy that details how it controls authentication and access to information.

Chelmsford County High School for Girls

2.26 Does the school have a policy that details how it requires all staff to create and manage passwords for all their devices, systems, and services?	No	Non-compliant		The school should consider formalising a written policy that details how staff should create and manage passwords.
If yes...	[redacted]			
- Does this policy ensure all users always use a password of at least 8 characters?				
- Does this policy stipulate that systems controlled by the school don't restrict the length of passwords?				
- Does this policy require users to change their password if they believe it has been compromised?				
- If yes, please explain how this is achieved.				

Chelmsford County High School for Girls

2.27 Is it school policy to require its suppliers to meet a set of security requirements?	Yes	**Compliant**	[redacted]
- If yes, please explain these requirements	Data Privacy Impact Assessments in place for all new suppliers, which must be approved by DPO before implementation. This includes security requirements.	**Compliant**	
2.28 How are all your school's relevant information security policies distributed to all employees?	Part of new joiners pack and all available on shared staff drive	**Compliant**	

Chelmsford County High School for Girls

Section 3 - Information Assets & Risk Management			
3.1 Is all sensitive information in your school identified and protectively marked?	No	**Non-compliant**	The school should consider creating an asset register for information assets (physical, people and data) that details their security requirements, owner, location and informs risk assessments. Sensitive information should be identified and protectively marked.
3.2 Does your school have an asset register that includes information assets?	Yes	**Compliant**	
If yes...			
- Does the register record the owner for every information asset?	Yes	**Compliant**	
- Does the register track the location of every information asset?	Yes	**Compliant**	
- Does the register record whether the information asset is password protected?	No	**Non-compliant**	The school should consider creating an asset register for information assets (physical, people and data) that details their security requirements, owner, location and informs risk assessments.

Chelmsford County High School for Girls

- Does the register record whether the information asset is encrypted?	No	**Non-compliant**		The school should consider identifying and recording encrypted information assets in the asset register.
3.3 Are all information assets securely deleted or disposed of when no longer required?	Yes	**Compliant**		
3.4 Does your school document the inward and outward flow of all sensitive information, including personal data?	Yes	**Compliant**		
If yes...				
- Does the data flow documentation include where the data was collected?	Yes	**Compliant**		
- Does the data flow documentation include where the data is stored?	Yes	**Compliant**		

- Does the data flow documentation include the destination for the data?	Yes	**Compliant**	[redacted]

Chelmsford County High School for Girls

Section 4 - Managing Cloud Services			
4.1 Has your school identified and recorded all cloud service providers that process its data?	Yes	**Compliant**	
If yes...			
- Does your school also record the security accreditations that are held by the provider?	Question not answered	**Non-compliant**	The school should consider recording the security accreditations (for example ISO 27000) held by the cloud service provider, especially if sensitive information is stored in the cloud.
- Does your school also record whether the data is encrypted in transit?	Question not answered	**Non-compliant**	Data transmission between school systems and the cloud provider must be done over a secure channel (for example, by using TLS). The school should consider keeping a record of this.
- Does your school also record whether the data is encrypted at rest?	Question not answered	**Non-compliant**	The school should consider confirming with the cloud service provider if the school's data is encrypted at rest.

Chelmsford County High School for Girls

4.2 Does your school use cloud service providers to share information with employees, pupils or parents?	Yes	**Compliant**	[redacted]
4.3 Does your school identify and record where all cloud service providers store its data?	Yes	**Compliant**	

Chelmsford County High School for Girls

Section 6 - People				
6.1 When your school recruits staff does it take up references and confirm employment history according to safeguarding directives?	Yes	**Compliant**	[redacted]	
6.2 Does your school always perform criminal record checks when recruiting staff?	Yes	**Compliant**		
6.3 When your school recruits staff, does it include cyber security and data protection responsibilities training in the staff member's induction?	Question not answered	**Non-compliant**	Including cyber security and data protection responsibilities within the staff induction process could encourage compliance with policy and practises.	The school should consider formal cyber security awareness training as part of the staff member induction process.
6.4 Do all staff receive at least annual cyber security awareness training?	Question not answered	**Non-compliant**	[redacted]	The school should consider a formal staff and board member cyber security awareness programme that allows for monitoring and recording performance.
6.5 Do all staff receive at least annual data protection awareness training?	Yes	**Compliant**		

Chelmsford County High School for Girls

6.6 Do staff know the route to follow to report information security incidents without recrimination?	Yes	Compliant	[redacted]
- If yes, are incidents always recorded and investigated?	Yes	Compliant	
6.7 Are staff made aware that they are not allowed to install software or code on the school's computers without permission?	Yes	Compliant	
- If yes, are staff that install software or code without permission subject to disciplinary action?	Yes	Compliant	

Chelmsford County High School for Girls

6.8 Does the school include cyber security responsibilities and adherence to information security policies within staff employment contracts?	Yes	Compliant	[redacted]
6.9 When staff leave the school are their accounts disabled or deleted?	Yes	Compliant	
6.10 Are staff only given enough privileges on IT systems that they require to do their job?	Yes	Compliant	

Chelmsford County High School for Girls

Section 7 - Cyber Security Policy			
7A.1 Does your school always install and enable firewalls at the boundaries between the internal network and the internet?	Yes	Compliant	[redacted]
- If yes, when being installed are all default passwords including the administrative account password always changed?	Yes	Compliant	
- If yes, is this password always at least 8 characters in length and difficult to guess?	Yes	Compliant	

Chelmsford County High School for Girls

7A.2 When configuring a new firewall password, which one of the following requirements do you follow?	A password with a minimum length of 12 characters and no maximum length	**Compliant**	[redacted]
- If other, please describe the requirements.	[redacted]		
7A.3 Do all school or user-owned (BYOD) devices that externally access school data or services do so through a virtual private network (VPN)?	No	**Compliant**	
- If no, are host-based firewalls always enabled on these devices?	Yes	**Compliant**	

Chelmsford County High School for Girls

7A.4 Does your school have any internal applications or services that are accessible externally through your network boundary?	Question not answered	**Non-compliant**	This area could not be assessed as the question was left unanswered.	[redacted]
If yes...	[redacted]			
- Do any of these applications or services provide sensitive information (that shouldn't be made public) to external users across the internet?				
- Do these applications or services lock user accounts or IP addresses out after ten or fewer unsuccessful login attempts or limit the number of login attempts to no more than ten within five minutes?				

Chelmsford County High School for Girls

- Does each of these applications or services have a documented business case?	[redacted]	
- If yes, is there a process for ensuring that they are disabled in a timely manner when they are no longer required?		
7A.5 Are all network boundary firewalls set to deny all other services than those permitted from being advertised to the internet?	Yes	**Compliant**

Chelmsford County High School for Girls

7A.6 Are any network boundary firewalls configured to be administrated over the internet?	Yes	**Compliant**	
If yes...			
- Is there a documented business case for this?	No	**Non-compliant**	The school should consider creating a formal business case whenever there is a business need for network boundary firewalls to be configured over the internet as this could be considered high risk.
- Is this access permitted only to trusted public IP addresses?	Yes	**Compliant**	
- If no, are all user accounts secured with multi-factor authentication?			

Chelmsford County High School for Girls

7A.7 Are all software firewalls (host-based) always enabled on all the school's computers (including thin clients), laptops and servers?	Yes	**Compliant**	[redacted]
- If no, please explain the reason why. Please list operating systems that don't have firewalls installed by default, if any.	[redacted]		
7B.1 Does your school always remove software that isn't required on laptops, computers, servers, thin clients, tablets and smartphones?	Yes	**Compliant**	
- If yes, please explain how this is achieved.	Reinstall all new machines with school image, which contains minimal software Windows and office 365). only deploy software based on department/user. All machines get reinstalled when they change user.	**Compliant**	

7B.2 Does your school always remove local user accounts that aren't required on laptops, computers, servers, tablets, smartphones and cloud services?	Yes	**Compliant**	[redacted]
- If yes, please explain how this is achieved.	Reinstall with school image to ensure that the only local account in the administrator account set with the schools local admin password.	**Compliant**	
7B.3 Does your school always change the default password for all user and administrative accounts on its laptops, computers, servers, tablets, thin clients and smartphones?	Yes	**Compliant**	
- If yes, is this password always at least 8 characters in length and difficult to guess?	Yes	**Compliant**	

7B.4 Is "auto-run" or "auto-play" for removable media and disk images disabled on all of the school's systems?	Yes	**Compliant**	[redacted]
7B.5 Does your school use device unlocking credentials to grant access to software and services on devices that require a user to be present? *For example, Windows Hello or any similar technology that requires either using biometrics, at least at least a 6-character or a strong and password.*	Yes	**Compliant**	
If yes, which methods are allowed? (Tick all that apply)	Strong and unique password	**Compliant**	
How is this authentication protected against brute-forcing? *For example, by throttling of failed login attempts or locking devices after no more than 10 unsuccessful attempts)*	Accounts locked after 5 failed login attempts. Currently automatically unlocks after 30 minutes.	**Compliant**	

Chelmsford County High School for Girls

7C.1 Are all operating systems and firmware installed on the school's devices in current support by the vendor and eligible to receive fixes for security problems?	Yes	Compliant	[redacted]
7C.2 Are all software applications installed on the school's devices in current support by the vendor and eligible to receive fixes for security problems?	Yes	Compliant	
If no, have the devices with unsupported software installed been segregated into a separate network (or VLAN) and blocked from accessing school data and the internet?	[redacted]		
If yes, how is this achieved?			

Chelmsford County High School for Girls

7C.3 Is all software - including operating systems - licensed in accordance with the publisher's recommendations?	Yes	Compliant
7C.4 Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release?	Yes	Compliant
7C.5 Are automatic updates enabled for all operating systems?	Yes	Compliant
If no, please explain how high-risk or critical security updates for operating systems are installed within 14 days of release.		

Chelmsford County High School for Girls

7C.6 Are all high-risk or critical security updates for software applications installed within 14 days of release?	Yes	**Compliant**		
7C.7 Are automatic updates enabled for all software applications?	Yes	**Compliant**		
If no, please explain how high-risk or critical security updates for software applications are installed within 14 days of release.				
7C.8 Have you removed all software applications from your school's computers, laptops, servers, tablets and smartphones that are no longer supported to receive regular fixes for security problems?	No	**Non-compliant**		All software applications that are no longer supported by the developer must be uninstalled. Unsupported software that doesn't receive updates pose a severe cybersecurity risk to the school.

Chelmsford County High School for Girls

If yes, please explain how this is achieved.		
7D.1 Are users only provided with user accounts after a process has been followed to approve their creation?	Yes	**Compliant**
- If yes, please explain how this is achieved.	HR Department informs the IT department once all the paperwork and signed contract has been returned by the employee. Once this has been recived, IT then start the new user process.	**Compliant**

Chelmsford County High School for Girls

7D.2 Can staff only access laptops, computers and servers by entering unique credentials that only they know? (Are you able to confirm that there are no shared accounts in use by staff to access laptops, computers or servers?)	Yes	**Compliant**	
7D.3 Is there a process for giving someone access to systems at an "administrator" level?	Question not answered	**Non-compliant**	The school should consider formalising a process for giving someone 'elevated privileges' to computer systems. This should be approved by the board.
- If yes, please describe this process.			

Chelmsford County High School for Girls

7D.4 Do administrators only use their administrator-level accounts to carry out administrative activities?	Yes	**Compliant**	
- If yes, please explain how this is enforced.	All daily accounts are standard user accounts. Need to login as a different admin account if a task requires administrator rights. Log out once finished and use daily standard account.	**Compliant**	
7D.5 Does your school formally record which users have administrator-level accounts?	Question not answered	**Non-compliant**	The school should maintain a 'Special Privileges Register' that records users with higher level privileges, the justification for high privileges and should be reviewed at least annually.

Chelmsford County High School for Girls

- If yes, is this record reviewed at least annually?	[redacted]	
- If yes, please explain how this is achieved.		
7D.6 Does your school have multi-factor authentication enabled for access to all administrator-level accounts?	Question not answered	Non-compliant

Chelmsford County High School for Girls

- If no, is a record kept of all systems that do not support multi-factor authentication?	[redacted]	
7D.7 Does your school have multi-factor authentication enabled for all users on all your cloud services?	Yes	Compliant
If no, please list the any of your cloud services that do not support multi-factor authentication.	[redacted]	

Chelmsford County High School for Girls

7D.8 Please explain how users are guided to choose strong and unique passwords.	Group policy forced, Paragraph about passwords in new staff induction document. Instructions on automated password reminder email. Students told during first computer science lesson, where they are given there logon details, and change the password during the lesson.	**Compliant**	[redacted]
7D.9 When you deploy wireless and wired networks, do you ensure that access is restricted only to authorised users?	Yes	**Compliant**	
- If yes, please explain how this is achieved.	Locked WiFi networks & wired - only accessible via password	**Compliant**	

Chelmsford County High School for Girls

7E.1 Which of the following does your school include in its strategy for protection against malware? (Tick all that apply)	Having anti-malware software installed. Limiting installation of applications to an approved set only (application allow-listing)	**Compliant**	[redacted]
7E.2 Do all computers, laptops and servers in the school have anti-malware software installed?	Yes	**Compliant**	
If yes...	[redacted]		
- Is it configured to update daily?	Yes	**Compliant**	
- Is it configured to scan files automatically upon access?	Yes	**Compliant**	

Chelmsford County High School for Girls

- Is it configured to scan web pages automatically upon access?	Yes	**Compliant**	[redacted]	
7E.3 Does your school prevent the installing of applications that aren't approved by restricting to only signed applications or those downloaded from an app-store?	No	**Non-compliant**	It is important to maintain a register of approved software. No software or apps should be installed on school computers that are not included on this list.	The school should consider preventing unsigned and unapproved applications from being executed on devices.
- If yes, do you have a documented list of approved applications?	[redacted]			
- If no, do you restrict installation to only signed applications or those downloaded from an app-store?				
7E.4 Does your school use sandboxing as a protection against malware on any systems?	No	**Compliant**		

Chelmsford County High School for Girls

- If yes, do you ensure that applications inside the sandbox are unable to access data, sensitive peripherals and the local network?	[redacted]	
- If yes, please explain how this is achieved.		
7F.1 Are data stored on the school's premises backed up at least weekly?	Yes	Compliant
If yes...		
- Are backup copies stored in a different geographical location?	Yes	Compliant

Chelmsford County High School for Girls

- Are in-progress backup data encrypted in transit?	Yes	**Compliant**	[redacted]
- Are backup copies of data stored with at least the same level of security as their origin?	Yes	**Compliant**	
7F.2 How much data (in terabytes) does your school store on-premises?	Approximated 9Tb for whole server enviroment.	**Compliant**	
7G.1 Does your school have a mechanism for alerting the technical team when there are indications ransomware is modifying data?	Question not answered	**Non-compliant**	It is important to implement a method that quickly detects ransomware attacks and alerts the technical team, so that incidents can be contained, and damage limited.
7G.2 Does your school review event logs at least weekly? (this can include automated system log monitoring software)	Yes	**Compliant**	

Chelmsford County High School for Girls

7G.3 Does your school ensure that event log information is kept secure and not leaked to unauthorised users?	Question not answered	**Non-compliant**	Event log information can be sensitive and should not be leaked to unauthorised users.	The school should consider formalising its cyber security intentions through written policies that identify standards, responsibilities and provide accountability.
7G.4 Is an audit trail of system and data access by staff maintained in a central location for all relevant systems and reviewed on a regular basis?	Question not answered	**Non-compliant**	It is good practice to have a centralised location for system and data access logs to ease security incident investigations and anomaly identification	The school should consider formalising its cyber security intentions through written policies that identify standards, responsibilities and provide accountability.
- If yes, please explain how this is achieved.	[redacted]			
7G.5 Does your school ensure that all devices have their time set accurately with the same source to ensure logs and audit trails are in sync?	Yes	**Compliant**	[redacted]	

Chelmsford County High School for Girls

Section 8 - Change Management			
8.1 Does the school ensure that all new and modified IT equipment and software applications include appropriate security provisions and comply with its own security requirements?	Yes	Compliant	[redacted]
8.2 Does the school ensure that all new and modified IT equipment and software applications are appropriately sized?	Yes	Compliant	
8.3 Before IT equipment and software applications are installed or modified, are they risk assessed and segregated with appropriate security controls if identified as critical?	Yes	Compliant	

Chelmsford County High School for Girls

8.4 Are significant changes to IT systems, software applications or networks always reviewed and approved in advance?	Yes	**Compliant**	[redacted]	
- If yes, please explain how this is achieved.	Question not answered	**Non-compliant**	[redacted]	The school should consider having a formalised and documented risk-based approach to reviewing and approving significant IT changes.

Chelmsford County High School for Girls

Section 9 - Security Testing, Audit & Assurance				
9.1 Does your school have vulnerability scans performed on its IT systems?	Question not answered	**Non-compliant**	[redacted]	The school could consider conducting regular IT vulnerability scans to expose risks and measure conformance to policy.
If yes...	[redacted]			
- Do the scans identify and report on how the school can improve security?				
- Does the school carry out penetration testing on critical school business?				

Chelmsford County High School for Girls

Section 10 - Incident Management, Continuity & Recovery			
10.1 Has your school defined what it considers a cyber security incident?	Yes	Compliant	[redacted]
10.2 If required as a result of a cyber security incident, is data isolated to preserve for forensic examination?	Yes	Compliant	
10.3 Is a record kept of the outcome of all security incident investigations to ensure all lessons have been learned from each event?	Yes	Compliant	
10.4 Do all staff involved with incident management have clear roles?	Yes	Compliant	
- If yes, have all staff with these roles received appropriate training to carry them out effectively?	Yes	Compliant	