IASME & Cyber Essentials Combined Scheme

Applicant: Changing Education Limited,

Thank you for applying for certification to the IASME & Cyber Essentials Combined Scheme Self-Assessment.

Congratulations, you have been successful in your assessment under the Cyber Essentials scheme.

Congratulations, you have been successful in your assessment for the IASME standard and successful in assessment against GDPR.

I include below the results from the form which you completed.

Question	Answer	Score	Comments
Acceptance Please read these terms and conditions carefully. Do you agree to these terms? NOTE: if you do not agree to these terms, your answers will not be assessed or certified.	I accept	Compliant	
A1.1 Organisation Name What is your organisation's name (for companies: as registered with Companies House)? Please provide the full name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity.	Changing Education Group	Compliant	
A1.2 Organisation Number What is your organisation's registration number (if you have one)? If you are a UK limited company, your registration number will be provided by Companies House, in the Republic of Ireland, this will be provided by Companies Registration Office. Charities, partnerships and other organisations should provide their registration number if applicable.	06677456	Compliant	
A1.3 Organisation Address Where are you located? Please provide the legal registered address for your organisation, or your trading address if a sole trader.	UK Address Line 1: 67 Kingsleigh Road, Town/City: Stockport, Postcode: SK4 3PP	Compliant	
A1.4 Type of Organisation What is your main business? Please summarise the main occupation of your organisation.	Education Applicant Notes: 85600 - Educational support services	Compliant	
A1.5 Website What is your website address? Please provide your website address (if you have one). This can be a Facebook/Linkedin page if you prefer.	https://changingeducation.co.uk	Compliant	

Question	Answer	Score	Comments
A1.6 Size of Organisation What is the size of your organisation? Based on the EU definitions of Micro (<10 employees, < €2m turnover), Small (<50 employees, < €10m turnover) , Medium (<250 employees, < €50m turnover) or Large (>250 Employees or >€50m turnover).	Small (<50 Employees and <€10m Turnover)	Compliant	
A1.7 Home Workers How many staff are home workers? Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when travelling.	Home workers - 11 The College is closed to all staff, students and partners.	Compliant	
A1.8 Certification Renewal Is this application a renewal of an existing certification or is it the first time you have applied for certification?	New Application	Compliant	
A1.9 Reason for Certification What is your main reason for applying for certification? Please let us know the main reason why you are applying for certification. If there are multiple reasons, please select the one that is most important to you. This helps us to understand how people are using our certifications.	Other Applicant Notes: Client requirement Competitive advantage	Compliant	
A2.1 Assessment Scope Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer 'No' to this question you will not be invited to apply for insurance. Your whole organisation would include all divisions and all people and devices that use business data.	Yes	Compliant	

Question	Answer	Score	Comments
A2.3 Hold Personal Data Does your organisation hold or process personal data (as defined by your country's data protection legislation)? You can find details of the definition of personal data at your country's government data protection website (in the UK, this is www.ico.org.uk. In the Republic of Ireland this is www.dataprotection.ie)	Yes	Compliant	
A2.4 EU GDPR Is your usage of personal data subject to the EU GDPR? If you process personal data about residents of the European Economic Area (EEA), you must comply with the EU GDPR wherever you are located in the world.	Yes	Compliant	
A2.5 Geographic Location Please describe the geographical locations of your business which are in the scope of this assessment. You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores).	All UK Offices	Compliant	
A2.6 Devices Please provide a summary of all laptops, computers and servers that are used for accessing business data and have access to the internet (for example, "We have 25 laptops running Windows 10 Professional version 1709 and 10 MacBook Air laptops running macOS Mojave"). You do not need to provide serial numbers, mac addresses or further technical information. **It is essential to include the Edition and Version number for Windows 10** - the assessor will be unable to mark the assessment without this.	as attached	Compliant	Confirmed that they are running Windows 10 Home

Question	Answer	Score	Comments
A2.7 Mobile Devices Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system version for all devices. All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information.	Mobile devices are used for telephone calls only and are not used for accessing emails or any other company applications.	Compliant	
A2.8 Networks Please provide a list of the networks that will be in the scope for this assessment. You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information.	Main network at office address	Compliant	
A2.9 Network Equipment Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You should include all equipment that controls the flow of data such as routers and firewalls. You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic.	Whilst the organisation has access to a wifi network provided by the college, all members of staff are currently working at home and the organisation is reliant on home networks. To reduce the risk, the organisation has enabled all software firewalls and has provided instructions and received confirmation that all default passwords have been amended.	Compliant	

Question	Answer	Score	Comments
A2.10 Responsible Person Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment? This should be the person who influences and makes decisions about the computers, laptops, servers, tablets, mobile phones and network equipment within your organisation. This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.	Stephen Hackney - Director	Compliant	
B1.1 Security Responsibility Please provide the name of the board member/director/partner/trustee who has responsibility for information security and data protection. This person must be a leader within your organisation who takes full responsibility for information security and data protection. This person cannot be an employee of an outsourced IT provider. You can name multiple people if required.	Stephen Hackney (Director)	Compliant	
B1.2 Standing Agenda Item Is information security and data protection (including a review of any recent incidents) a standing agenda item for your board/director/partner/trustee meetings? It is vital that the board/owners of the organisation are involved in information security and data protection	Yes Applicant Notes: Yes - discussed as part of team reviews etc	Compliant	
B1.3 Overall Responsibility Please provide the name and role of the person who has overall responsibility for managing security in your organisation. This person must have day-to-day responsibility for operational security within your organisation.	Stephen Hackney (Director)	Compliant	

Question	Answer	Score	Comments
B1.4 Skills and Funding How do you ensure that you provide sufficient funding and a suitable number of appropriately skilled staff to develop and maintain good information security and data protection? To ensure that your organisation remain secure, you need to prioritise funding for security and data protection initiatives and ensure that you have suitable skills within the organisation.	Yes - funding provided and contract in place with an external 3rd party provider to deliver additional support for GDPR etc	Compliant	
B2.1 Asset Registers Does your organisation have up-to-date information and physical asset registers? An asset register should track all categories of information and provide an owner for each one. It links closely to risk assessment by identifying the information assets that are to be protected. IASME has an information asset register template that can be used by applicants.	Yes Applicant Notes: Yes - hardware and software register in place. Software inventory contains a list of all 3rd party software that is used.	Compliant	
B2.2 Information Asset Tracking How does your asset register track information assets (i.e. categories of information)? An information asset might be a set of data (for example 'employee information') which will have a location attached to it (for example 'the server in the HR department') and an owner (for example the 'HR director').	As part of the IASME process a full data map / ROPA has been created with owners identified for each of the individual assets	Compliant	
B2.3 Named Owners Do all assets (both physical and information assets) have named owners? Having a named owner ensures that someone is taking responsibility for each asset.	Yes Applicant Notes: Every machine is set up by IT leader - each device has an owner assigned. Admin password is stored in 1Password. Users have ontrol of their own passwords and updates are scheduled	Compliant	

Question	Answer	Score	Comments
B2.4 Removable Media Is all removable media tracked in the asset register and encrypted? Please describe how you achieve this. Removable media includes USB sticks, USB hard drives and DVDs/CDs. It might also include backup tapes. You need a list of all removable media you use and need to manage how it is used, where it is used and by whom.	Information and Security Policy in place stated that no external hard drives should be in used - this is reinforced in the HR Manual	Compliant	
B2.5 Mobile Phones Are all mobile phones, tablets and laptops tracked in the asset register, pin/ password protected and encrypted? Please describe how you have achieved this for all criteria within this question. This can be achieved using built-in tools (such as iCloud/Find my iPhone, Find my Android or additional mobile device management (MDM) software.	No mobile phones in scope or tablets. Own phones are used for telephone calls only. No data is stored on their phones or access to the WhatsApp groups	Compliant	
B2.6 Data Identified Is all personal data and special category data identified (e.g. by protective marking) and properly protected? Describe how this is done. You need to be able to identify any such data within your organisation. This is important to ensure the rights of data subjects are upheld and will assist with meeting requirements such as Subject Access Requests.	This is contained in the Data Map / ROPA. All information held by the organisation is considered to be confidential	Compliant	
B2.7 Documented Data Flows How do you ensure all flows of personal and special category data are documented, including where data was obtained, where it is stored and all destinations of data? You must be able to show how such data flows into and through your company. Using a diagram can be a useful way to achieve this requirement.	This is contained in the Data Map / ROPA which identifies where the data was captured, where it is stored, who it will be shared with, retention periods, delete processes etc	Compliant	

Question	Answer	Score	Comments
B2.8 Sensitive Information Identified Is all sensitive information identified (e.g. by protective marking) and properly protected? You must be able to identify all sensitive information within your company and make sure it is protected from cyber threats and errors/staff mistakes. You can do this by using protective marking where you assign categories (public, confidential, secret) and mark these categories on documents, emails and spreadsheets. You don't have to use protective marking if you have other ways to keep sensitive information identified and protected.	Yes Applicant Notes: Yes - sensitive data may belong to users of the service relating to their placement eg. medical information to allow suitable adjustments to be made. This is highlighted in the privacy policy as being sensitive together with agreements with Education providers	Compliant	
B2.9 Secure Destruction When assets are no longer required, is all data securely wiped from them or are the assets securely destroyed? Describe how this is done. 'Assets' include laptops, servers, tablets, USB hard drives and USB sticks. Special software can be used to securely delete data or external companies can be used to provide a secure destruction service. You can alternatively physically destroy the assets yourself, although this is not always effective.	To be destroyed - old hard drives are either physically destroyed. 3rd party arrangement with Air Ambulance is being investigated who are CESG qualified	Compliant	
B2.10 Cloud Providers Do you use cloud providers to store company information (such as files, emails, data backups)? If so, please list all providers. Most companies will use at least one cloud provider to store data which could include file storage such as Dropbox, emails using Office365 or Gsuite, and cloud backup providers	"Gsuite. WhatsApp. GoogleMeets & Zoom used for comms Connect (online platform), Studetn App for workplacement, API to allow platofrms toalk together on AWS and PostMark. Comms for employer and students via Postmark Monday.com used for CRM, Code in GitHu, Comms via Slack Sage1 Cloud Accountancy, Accountancy store data for HR purposes with payroll info sent to accoutns, Mailchimp for Client data.	Compliant	

Question	Answer	Score	Comments
B2.11 Share Information Do you use cloud providers share company information between employees or with customers (such as instant messaging or collaboration tools)? If so, please list all providers. Cloud providers that your use to share information could include Slack, Yammer, Teams, Gsuite, Jira, Confluence and Basecamp.	Gsuite, DocuSign and Mailchimp used for Comms.	Compliant	
B2.12 Provider Location Where do your cloud providers store your data? You should provide the geographical location or region (for example UK, USA, European Union, or China) for all your cloud providers, using a list if needed.	AWS in Ireland, GitHub - US. Website is UK - ready to be hosted elsewhere. Some 3rd parties (eg. Postmark) transfer data to the US	Compliant	
B2.13 GDPR Provisions Please describe which provisions have been put in place to ensure that the requirements of the GDPR are met fully for the data held in your cloud services? If your cloud providers store your data outside of the European Economic Area (EEA) you will need to check that they have signed up to rules or agreements that ensure they offer equivalent protection to your data as would be found within the EEA.	A review of all providers post Schrems II has identified that all use SCC's or BCR's instead of Privacy Shield. Risk added to Risk Register re. the need for additional checks on provider which are yet to be determined / outlined by the ICO.	Compliant	
B2.14 Security Accreditations Which security accreditations are held by the cloud providers used by your organisation? Your cloud providers should hold suitable security accreditations, particularly if you store sensitive data with them. Examples of security accreditations include ISO27001 and G-cloud.	ISO27001 / SOC2 etc. All providers have been validated as part of the Asset Management process.	Compliant	

Question	Answer	Score	Comments
B2.15 Encrypted in Transit Is your data encrypted before being passed between your site and your cloud provider(s) (i.e. encrypted in transit)? Your cloud provider must encrypt your data when it is being sent between your computers and the cloud provider. This is usually achieved by using TLS encryption. For web-based services look for the https:// in the address bar and a padlock icon.	Yes Applicant Notes: Providers encrypt at rest and in transit. Changing Education use TLS encryption	Compliant	
B2.16 Encrypted at Rest Is your data encrypted whilst being stored by your cloud provider(s) (i.e. encrypted at rest)? Your data should be encrypted by your cloud provider when it is being stored on their systems. It is difficult to confirm this just by looking at the cloud service - you will need to contact you cloud provider or view their security documentation to confirm this.	Yes Applicant Notes: As above	Compliant	
B3.1 Current Risk Assessment Do you have a current Risk Assessment which includes information security risks and includes risks to data subjects for the information you hold? You must ensure that your risk assessment covers risks to data from events such as malware infection, criminal activity and staff making mistakes. If you already use a risk tool for topics such as health and safety risks or other business risks, you can expand this to include information risks. A template is available from IASME.	Yes Applicant Notes: A full risk register has been developed which considers risks across the organisation including information security risks,	Compliant	
B3.2 Risk Assessment Reviewed Has your risk assessment been reviewed in the last 12 months? Who reviewed it? The assessment must be reviewed by a suitable group of people who between them have knowledge of all areas of the organisation.	Reviewed and updated in August 2020 by the Directors. Reviewed on a 6 monthly basis.	Compliant	

Question	Answer	Score	Comments
B3.3 Risk Assessment Cover Scope Does the risk assessment cover the scope of this assessment? The risk assessment should cover the scope of your IASME Governance assessment.	Yes Applicant Notes: Full scope risk assessment	Compliant	
B3.4 Risk Actions Does the risk assessment identify which actions you will be taking for each risk (such as reduce or accept)? You need to make a decision for each risk you identify what you intend to do about it. Usually you will choose to decide the risk by making changes to your systems or processes.	Yes Applicant Notes: Owners are identified where appropriate	Compliant	
B3.5 Action Plan Do you have an action plan to implement any actions identified in the risk assessment? An action plan lets you priorities the changes that are needed to reduce the risks identified in your risk assessment.	Yes Applicant Notes: Actions have been identified for each risk where appropriate	Compliant	
B3.6 Approval Was the risk assessment approved at board/director/partner/trustee level? Your risk assessment must be signed off and the person who signs off must agree to accept the risks that will remain after your action plan is implemented.	Yes Applicant Notes: Yes - approved by Stephen Hackney and Matt Hodgkinson	Compliant	
B4.1 Mitigate Risks Have you put policies and procedures in place to mitigate risks to personal data? To effectively manage risks to personal data you need a set of policies that set out your expectations and requirements around handling personal data.	Yes Applicant Notes: A detailed Information Security & Privacy Policy is in place which links to the HR Handbook.	Compliant	

Question	Answer	Score	Comments
B4.2 Everyday Practice Are these policies and procedures provided to all employees, required to be followed in everyday practice and linked to disciplinary procedures? How do you achieve this? It is important that the policies and procedures are followed by all employees in all situations.	The policy has been cascaded as part of the process to introduce a new HR Handbook to the organisation. All staff have now received the new handbook.	Compliant	
B4.3 Contracts of Employment Is Data Protection referred to in employee contracts of employment? Employee contracts of employment should outline responsibilities for the handling of the personal data of customers and employees.	Yes Applicant Notes: Included in the contract and reinforced in the HR Handbook.	Compliant	
B4.4 Clear Responsibilities Do policies and procedures set clear responsibilities for handling of personal data, including where appropriate reference to responsibilities held by your Data Protection Officer? Those in your organisation who handle personal data should clearly understand their responsibilities. If you have a data protection officer, they will play a key part in making people aware of their responsibilities.	Yes Applicant Notes: These is clearly documented in the Info Sec & Privacy document, and reinforced in the HR Manual.	Compliant	
B4.5 Data Protection Officer If you fall into the category of requiring a Data Protection Officer have you appointed one? The GDPR introduces a duty for you to appoint a data protection officer if you are a public authority or body, or if you carry out certain types of processing activities.	No Applicant Notes: There is no requirement within the organisation for a DPO however Stephen Hackney is the Data Officer	Compliant	

Question	Answer	Score	Comments
B4.6 Collection Purposes When your organisation collects personal data from a subject do you clearly state what it is being collected for, how it will be processed and who will process it and does the data subject have to provide consent for this? You must state why you are collecting personal data clearly at the point of collection.	Yes Applicant Notes: "This is clearly documented in the Data Privacy Policy which is available on the company website. A DPIA can be shared with Clients which clearly outlines that Changing Education is a Data Processor and that responsibilty for consent is with the Education Provider, For employees and other members of staff, an internal data privacy policy is available which provides a similar breakdown of information. Consent is used in a limited number of instances eg. consent for use of photographs as part of marketing. "	Compliant	
B4.7 Data from Children Where you collect data from children, do you actively seek parental consent? How do you record this? You must record consent clearly so that you can track it and can refer to it later as needed.	"As part of the sign up to a programme there is a parent al consent form this includes the need to share anything that could impact the success of the work placement (includes medical data eg. nut allergies, learning issues etc) so that the employer can make reasonable adjustments. However, the organisation is a data processor, the contract is clear that the Controller (ie. Education Providers) is responisble for gaining consent from the student or parent. "	Compliant	
B4.8 Data Requests What is your process for dealing with Subject Access or Data Portability requests within 30 days? Do you have processes in place to maintain the rights of the individual, within the time limits laid down by the Regulation? Under data protection legislation, individuals have a right to obtain a copy of the information you hold about them. This could include requests for subject access or data portability.	A subject access request procedure is available and is documented. If required, external support from a 3rd party consultant is available to support these requests.	Compliant	

Question	Answer	Score	Comments
B4.9 Contact Organisation Do you make it clear to data subjects how they should contact your organisation to exercise their rights and to raise complaints? Under data protection legislation, individuals have rights over the use of their data. It is important that the process that can be used to exercise these rights is clearly communicated to clients and other data subjects.	Yes - this is detailed on the privacy policy on the website for data subjects external to the organisation, and in the HR Handbook and Internal Data Privacy Policy.	Compliant	
B4.10 Retention Periods Do you have documented data retention periods and do these cover contractual and legal requirements? You should decide how long you need to keep each type of data once the justification for keeping it has expired (such as when a customer stops using your product). Retention period will be influenced by legal requirements and your business needs.	Yes Applicant Notes: These are documented in the Data Processing Map (records of processing). Lawful basis and appropriate retention periods are documented. This is available to all members of staff on request and to external 3rd parties	Compliant	
B4.11 Data Classification Criteria Do you have documented data classification criteria? Data classification allows you to prioritise your efforts in protecting data by clearly identifying the most sensitive data to your organisation. Classification categories might include 'public', 'confidential', 'sensitive' or 'secret'.	Yes Applicant Notes: The organisation considers all information within the organisation to be confidential with the exception of sensitive information which is labelled as sensitive.	Compliant	
B4.12 Data Privacy Statement Do you have a data privacy statement compliant with the requirements of GDPR and does the statement provide a point of contact for data protection issues? Who is the point of contact? A data privacy statement is an important document that sets out the justifications for your use or personal data. It should be made available to data subjects, often by hosting it on a company website.	This was reviewed and updated as part of the IASME process and is available on the company website for external readers and in the HR Handbook for members of staff. Stephen Hackney is the Data Officer for the organisation. Contact details have been provided	Compliant	

Question	Answer	Score	Comments
B4.13 Subject Consent Where you are holding data based upon the consent of the data subject, how do you record details of the consent? You must record consent clearly so that you can track it and can refer to it later as needed.	"Consent for student information is the responsibility of the education provider. Consent within the organisation is only required for photographs that would be used as part of PR / Marketing. Evidence of consent is saved on gSuite and then used as per agreement on consent form"	Compliant	
B4.14 Remove Consent Do you have mechanisms in place which make it as easy for the data subject to remove consent for the data processing under the consent lawful purpose? In order to respect the rights of data subjects, its is necessary to have clear mechanisms for revoking consent for data processing when a subject requests it.	Yes Applicant Notes: "For Students, the student file would be deleted as part of normal business as usual processing. For members of staff, photographs would be removed however the HR Handbook makes it clear that if items have been used on Social media, removal cannot be guaranteed. "	Compliant	
B4.15 Justification For each piece of personal information and special category data you hold, do you record the justification for obtaining it? Where is this recorded? Justifications for obtaining the information might include explicit consent, contract fulfilment, performing a public function, meeting a legal requirement or another legitimate interest. Justifications for obtaining special category (or sensitive personal data) could include specific consent, use for employment purposes or to meet a medical need.	These are documented in the Data Processing Map (records of processing). Lawful basis and appropriate retention periods are documented. This is available to all members of staff on request and to external 3rd parties	Compliant	
B4.16 Roles For each piece of personal information you hold, do you record whether your organisation is the data processor or the data controller? The roles of data processor are different to those of data controller and carry different responsibilities.	Yes Applicant Notes: These are documented in the Data Processing Map (records of processing). The role of processor or controller is clearly defined and documented. This is available to all members of staff on request and to external 3rd parties	Compliant	

Question	Answer	Score	Comments
B4.17 Supplier Roles In each contract you hold with suppliers and customers involving the processing of personal data, do you confirm whether you are the data controller or data processor? The roles of data processor are different to those of data controller and carry different responsibilities. It is important that suppliers and customers understand your role in each relationship.	Yes Applicant Notes: "In contracts with Clients, Changing Education are defined as processors for Student data unless the information is used for contract / billing purposes in which case they are controllers. Internally, Changing Education are data controllers. Contracts have been reviewed, including those with sub processors, and the role is clearly defined and documented on the data processing map. "	Compliant	
B4.18 Legitimate Interest Where you have decided to hold data under the lawful purpose of Legitimate Interest of the Controller or Third Party, have you completed the three-part Legitimate Interest test and kept a record of the results? The test is used to verify that you can successfully use legitimate interest as a reason to hold data.	Legit interest is not used as a lawful basis for processing,	Compliant	
B4.19 Protection Measures Where you disclose personal data to a supplier/provider does the contract explicitly impose the obligation to maintain appropriate technical and organisational measures to protect personal data in line with relevant legislation? It is important that contracts make clear your security expectations in relation to personal data.	Yes Applicant Notes: Yes. Contracts are in line with articles 28-32	Compliant	
B5.1 References Do you take up references or confirm employment history (or carry out any other pre-employment checks to meet regulatory requirements) when employing new staff? How do you do this? You should carry out checks when employing staff to verify their identity.	Yes - this is managed in conjunction with the HR partner.	Compliant	

Question	Answer	Score	Comments
B5.2 Criminal Records Where criminal record checks are carried out, do you ensure that explicit consent has been obtained from employees and that such checks are carried out for lawful purposes? You must ensure that you have consent for such checks and that you a have a legal basis for carrying them out.	Yes Applicant Notes: every member of staff has to be DBS Checked - UK CRB Ltd.	Compliant	
B5.3 Training and Awareness Responsibility Provide the name and role of the person responsible for security and data protection training and awareness. This person must have day-to-day responsibility for training within your organisation.	Stephen Hackney, Data Officer and co-Director	Compliant	
B5.4 Data Protection Training Do all staff and contractors receive regular information security and data protection training (at least annually)? Describe how this is done. Appropriate training ensures all staff and contractors understand how to act securely when handling company data. Training could be in-person, online or carried out remotely.	Yes - this was education delivered as part of the IASME implementation process how ever other information eg. useful links from Risk Evolves has been provided which includes signposting to free resources.	Compliant	
B5.5 New Employee Briefing Do you give new employees a briefing on their corporate and security responsibilities before, or immediately after employment, preferably reinforced by reference literature? How do you do this? You must brief staff on their security responsibilities. By providing literature such as a copy of the security policy or reference sheet staff can remind themselves of your requirements at a later date.	Yes - there is a new starters process plus the Information Security & Privacy policy is included in the HR Handbook	Compliant	

Question	Answer	Score	Comments
B5.6 Security Obligations Do employee contracts include security obligations (such as an obligation to comply with the security policy) and are reminders given at regular intervals? Contracts ensure there is a legal basis for your security requirements	Yes Applicant Notes: Yes - this is a key part of contracts and HR Handbooks Reminders are provided as documented above	Compliant	
B5.7 Qualifications and Training Are employees with responsibility for information security, or with privileged access to business systems, appropriately qualified and suitably trained? It is important that those who hold security roles or have access to important data are skilled and trained so that that don't make mistakes. Qualifications do not need to be formal and may be replaced by setting requirements on experience in a particular sector.	Yes Applicant Notes: Yes – this has been provided by a 3rd party organisation (Risk Evolves) with ongoing sessions scheduled throughout the year.	Compliant	
B5.8 Employment Termination On termination of employment, are user access privileges immediately withdrawn and the employee de-briefed on their post-employment confidentiality responsibilities? How do you do this? It is important that you remove access to systems when terminating employment - depending on the circumstances surrounding termination, you may choose to remove access immediately and not require employees to complete their notice period.	The 3rd party HR company responsible for exit management briefs employees on their ongoing requirement to maintain confidentiality. On notification of the employees resignation, details are passed to the IT team to remove access. Depending on the role, the individual may be placed on garden leave and will not therefore work their notice. In these instances, access is removed immediately.	Compliant	
B6.1 Information Security Policy Do you have a policy or a set of policies that cover information security? A Security Policy can be stand-alone or can be formed from a number of policies within your policy set, but it should set out your objectives for managing your security.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	

Question	Answer	Score	Comments
B6.2 Policy Review Have your policies been reviewed in the last 12 months? Your security policies must be reviewed by a suitable group of people who between them have knowledge of all areas of the organisation.	Yes Applicant Notes: The policy was reviewed in September and is scheduled for review in Sept 2021	Compliant	
B6.3 Policy Scope Do your information security policies cover the scope of this assessment? The policies must apply to all business units covered by this assessment.	Yes Applicant Notes: The policies cover the full scope of the company,	Compliant	
B6.4 Policy Approval Provide the name and role of the person who approved the policies? This person must be a leader within your organisation. You can name multiple people if required.	Stephen Hackney, Data Officer and co-Director	Compliant	
B6.5 Review and Consultation Is there a policy review and consultation process? Policies must be regularly reviewed and updated to ensure they stay current and reflect business requirements.	Yes Applicant Notes: The policy was reviewed in September by both Directors and included the HR Partner in the sign off process. As part of the education and consultation process, a team meeting was held to explain to staff why the changes were required.	Compliant	
B6.6 Intellectual Property Do your policies refer to intellectual property rights and legal requirements? Your policies should meet any legal requirements that apply to your organisation.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	

Question	Answer	Score	Comments
B6.7 Personnel Security Do your policies refer to personnel security? Your policies should cover how you ensure that staff and contractors identities are verified and any other personnel security checks such as vetting are carried out.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	
B6.8 Asset Management Do your policies refer to asset management (including removable media)? Your policies should define how you manage physical and information assets including procedures when new assets are acquired and when assets are no longer required.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook. Removalble media is not permitted within the organisation	Compliant	
B6.9 Access Management Do your policies refer to user authentication and access management? Your policies should detail how users are authenticated onto your systems and how you ensure access to systems is restricted to only authorised people.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook. This includes rules on password management, sharing of user ids etc,	Compliant	
B6.10 Physical and Environmental Do your policies refer to physical and environmental security? Your policies should cover your requirements on physical access to locations and systems, as well as any environmental requirements such as heating and cooling of equipment.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	
B6.11 Computer and Network Do your policies refer to computer and network security? Your policies should cover security of systems and networks.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	

Question	Answer	Score	Comments
B6.12 Acceptable Usage Do your policies refer to monitoring and acceptable usage of systems/data? Your policies should detail how your company carried out monitoring of data and system access and usage. They should also details what usage is acceptable so that staff understand for which purposes they may use systems.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook. Policy states that systems may be used. An Acceptable Use policy is included	Compliant	
B6.13 Malware and Intrusion Do your policies refer to security from malware and intrusion? Your policies should set requirements around how systems are to be kept safe from malware attacks and attempts by hackers to gain access to systems and data through network intrusion.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook. Patching on all devices must be performed plus an AV must be in use.	Compliant	
B6.14 Incident Management Do your policies refer to security incident management? Your policies should detail how your company will deal with security incidents.	Yes Applicant Notes: Individuals are asked to report all incidents - regardless of severity for investigation and management where appropriate. This includes 'near miss' events. A incident management process is in place.	Compliant	
B6.15 Business Continuity Do your policies refer to business continuity measures? Your policies should details how your company will deal with incidents that threaten the viability and operation of the business through invoking business continuity measures.	Yes Applicant Notes: A business continuity plan is in place and has been tested as part of the Lockdown process	Compliant	
B6.16 Home and Mobile Working Do your policies refer to home and mobile working? Your policies should set expectations around how staff should act when working at home or in other locations such as client sites or when travelling.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook. This includes a mobile working policy	Compliant	

Question	Answer	Score	Comments
B6.17 Handling Personal Data Do your policies refer to handling personal data (and, where appropriate, reference your data protection policy)? Your policies should set requirements around handling of personal data. This may be contained within a data protection policy.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook which includes the criticality of the need for data management within the organisation	Compliant	
B6.18 Policy Distribution Are your information security policies distributed to all employees? You must distribute a copy of your information security policy set (containing all the topics listed in the previous questions) to all employees. This could be a physical copy or via email/instant messaging. You cannot just place the policy in a shared area, unless employees also receive an email/instant message with a link to the shared area and a request to click the link and view the policies.	Yes Applicant Notes: There is a comprehensive Information Security And Privacy Policy in place which has been cascaded to staff and is incorporated in the HR Handbook.	Compliant	
B6.19 Contractual Obligations Are your information security policies part of all employees' contractual obligations? Staff must be contractually obligated to follow the requirements defined within your policies.	Yes Applicant Notes: Incorporated in the HR Handbook which is referenced in the employment contract	Compliant	
B6.20 Supplier Security Requirements Do the contracts with all your suppliers ensure that they meet a set of security requirements that you have defined around handling data and keeping information secure? Please explain the requirements you have set and the reasons why you have chosen them. The security requirements you define for your suppliers may be determined by your regulatory or business environment. For example, MoD supplier will be required to flow-down certain security requirements to their supply chain.	A supplier questionnaire is available for new supplier assessment however a review of all current suppliers has been conducted to ensure that they have security and privacy statements that meets or exceeds the requirements of the organisation eg. has CE, or ISO27001, has a statement on website etc.	Compliant	

Question	Answer	Score	Comments
B6.21 Sector-Specific Regulations List any business sector-specific regulations relating to risk treatment or information security which apply to your business. Such regulations might include the Financial Conduct Authority rules for regulated businesses.	none	Compliant	
B6.22 Related Laws List any local or international laws relating to risk treatment or information security which apply to your business. Such laws might include the UK Computer Misuse Act, data protection legislation or local privacy laws.	UK DPA, PECR, Computer Misuse Act, UK GDPR	Compliant	
B6.23 Credit Card Information Do you store credit card information? Credit card information includes card numbers (PANs), expiry dates and personal details relating to cardholders.	No	Compliant	
B7.1 Justified and Approved Are only authorised personnel who have a justified and approved business case given access to restricted areas containing information systems or stored data? How do you achieve this? You must ensure that access to systems is only provided to people who have a legitimate need to access this systems. This means you must restrict access any other people from accessing such systems using locks, alarms, security cages or any other form of physical access control.	Access to student information is restricted to Directors and technical team as part of problem resolution, HR information is accessed by Directors and HR Partner	Compliant	

Question	Answer	Score	Comments
B7.2 Physical Media Is the use of physical media on your systems controlled either by physical access restrictions or by a technical solution (such as by configuring devices to blocking USB storage devices)? You can restrict access to USB devices and removable storage through Windows Group Policy or through third-party tools such as Sophos Cloud. For servers, you may choose to restrict access to the device to only trusted individuals.	These are blocked from use.	Compliant	
B7.3 Physical Media Scanning Where indicated as necessary in your risk assessment, do you have dedicated machines to scan physical media for viruses and malware? If your risk assessment identifies a particular risk from removable media you may choose to dedicate computers to scanning incoming USB keys, drives and disks for viruses before allowing them to be used with your day-to-day systems.	Not required	Compliant	
B7.4 Environmental Conditions Are devices which require particular working conditions (such as heating and cooling) provided with a suitable environment within the guidelines set out by their respective manufacturers? How do you achieve this? Servers and networking equipment may need air conditioning to ensure they keep to a reliable operating temperature.	Not required	Compliant	
B7.5 Physical Protection Do all business premises have effective physical protection and, if indicated by a risk assessment, surveillance and monitoring? You should carry out a physical risk assessment to determine if any areas of your premises are at risk of being accessed by unauthorised people. If you find risks, you should install locks, access control, video monitoring, additional staff or other controls to reduce the risk.	Yes Applicant Notes: Landlord provides CCTV camera and restricted access to premises. Please note - All business systems are cloud based	Compliant	

Question	Answer	Score	Comments
A4.1 Firewalls Do you have firewalls at the boundaries between your organisation's internal networks and the internet? You must have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network.	Yes Applicant Notes: Yes – software firewalls are active on all machines.	Compliant	
A4.2 Change Default Password When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices? How do you achieve this? The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub) You can change the default password by logging into the web interface for the device (often located at 192.168.1.1 or 192.168.1.254)	Yes – password changed as part of the install process.	Compliant	
A4.3 Password Quality Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess? A password that is difficult to guess will be unique and not be made up of common or predictable words such as 'password' or 'admin', or include predictable number sequences such as '12345'.	Yes Applicant Notes: In line with guidance from the NCSC re complex passwords. Enforced as part of policy	Compliant	
A4.4 Password Management Do you change the password when you believe it may have been compromised? How do you achieve this? Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.	Yes – this can be managed centrally by the IT team through 1Password. Education has also been provided to the team on why changing passwords may be required.	Compliant	

Question	Answer	Score	Comments
A4.5 Services Enabled Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case? At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a VPN server, a mail server or a service that is accessed by your customers). This is sometimes referred to as 'opening a port'. You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer 'No'. By default, most firewalls block all services. The business case should be documented and recorded.	No	Compliant	
A4.7 Service Blocking Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet? By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.	Yes Applicant Notes: Yes – software firewalls in use on all machines. When in the office, the College manages the router and all service are blocked.	Compliant	
A4.8 Configuration Settings Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet? Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer 'no' to this question.	No	Compliant	

Question	Answer	Score	Comments
A4.11 Software Firewalls Do you have software firewalls enabled on all of your computers and laptops? You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for 'windows firewall'. On Linux try 'ufw status'. You can also use the firewall that may be provided by your anti-virus software.	Yes Applicant Notes: Yes – software firewalls in use on all machines.	Compliant	
A5.1 Remove Unused Software Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? Describe how you achieve this. To view your installed applications on Windows look in Start Menu, on macOS open Finder -> Applications and on Linux open your software package manager (apt, rpm, yum). You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use.	Yes – for all company owned devices a standard build is used which removes unwanted software at install. All staff are periodically asked to bring their devices to the Crewe office, to be checked over. At this point if any surplus software is noticed they are asked for it's business case. If a machine is owned by the company then they do not have administrator access to install software. I	Compliant	
A5.2 Necessary User Accounts Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business? You must remove or disable any user accounts that are not needed in day-to-day use on all devices. You can view your user accounts on Windows by righting-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using 'cat /etc/passwd'.	Yes Applicant Notes: Yes – only one user is allowed to access a single laptop. This is further enforced through policy that users must not share their devices with other individuals eg family members while working at home.	Compliant	

Question	Answer	Score	Comments
A5.3 Change Default Password Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more? A password that is difficult to guess will be unique and not be made up of common or predictable words such as 'password' or 'admin', or include predictable number sequences such as '12345'.	Yes Applicant Notes: Yes – this is part of the standard build process. All computers owned by CE have an administrator account that is not handed out, the password is stored in 1password and if needed is unlocked by by the IT Dept. Development systems are only accessibly by the development team	Compliant	
A5.4 Password Quality Do all your users and administrators use passwords of at least 8 characters? The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.	Yes Applicant Notes: Yes – enforced through 1Password and supported with education and policy	Compliant	
A5.5 Sensitive or Critical Information Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet? Your business might run software that allows people outside the company on the internet to access information within your business via an external service. This could be a VPN server, a mail server, or an internet application that you provide to your customers as a product. In all cases these applications provide information is confidential to your business and your customers and that you would not want to be publicly accessible. This question does not apply to cloud services such as Google Drive, Office365 or Dropbox. If you only use such services and do not run your own service you should answer no to this question.	No	Compliant	

Question	Answer	Score	Comments
A5.10 Auto-Run Disabled Is 'auto-run' or 'auto-play' disabled on all of your systems? This is a setting which automatically runs software on a DVD or memory stick. You can disable 'auto-run' or 'auto-play' on Windows through Settings, on macOS through System Preferences and on Linux through the settings app for your distribution. It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option you can answer yes to this question.	Yes	Compliant	
A6.1 Operating System Supported Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems? Please list the operating systems you use so that the assessor can understand your setup and verify that all your operating systems are still in support. Older operating systems that are out of support include Windows XP/Vista/2003, mac OS El Capitan and Ubuntu Linux 17.10	windows, and apple ios.	Compliant	
A6.2 Applications Supported Are all applications on your devices supported by a supplier that produces regular fixes for any security problems? Please summarise the applications you use so the assessor can understand your setup and confirm that all applications are supported. This includes frameworks and plugins such as Java, Flash, Adobe Reader and .NET	Gmail is used for email plus word, excel etc. The organisation has developed its own application. Other cloud based applications for accounting etc are used. No data is held on laptops	Compliant	
A6.3 Software Licensed Is all software licensed in accordance with the publisher's recommendations? All software must be licensed. It is acceptable to use free and open source software as long as you comply with any licensing requirements.	Yes	Compliant	

Question	Answer	Score	Comments
A6.4 Security Updates - Operating System Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how do you achieve this. You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.	All machines are set to automatically install updates	Compliant	
A6.5 Security Updates - Applications Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this. You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.	Any MS office software is automated through windows, but the majority of users are on google accounts so all software is online	Compliant	
A6.6 Unsupported Applications Have you removed any applications on your devices that are no longer supported and no longer received regular fixes for security problems? You must remove older applications from your devices when they are no longer supported by the manufacturer. Such applications might include older versions of web browsers, frameworks such as Java and Flash, and all application software.	Yes Applicant Notes: Yes - All staff are periodically asked to bring their devices to the Crewe office, to be checked over. At this point if any surplus software is noticed they are asked for it's business case. If a machine is owned by the company then they do not have administrator access.	Compliant	

Question	Answer	Score	Comments
B8.1 Documented Procedures Is management of computers and networks controlled using documented procedures that have been authorised? Describe how you achieve this. Changes to systems must be made following clear procedures that have been defined by the organisation.	Changes to systems are managed via the development procedures in conjucntion with the Directors., Changes have to be tested in the development environment before being promoted to live.	Compliant	
B8.2 New Systems Does the organisation ensure that all new and modified information systems, applications and networks include security provisions, are correctly sized, comply with security requirements, are compatible with existing systems and are approved before they commence operation? Describe how you achieve this. You must incorporate security provisions into your decision making about new systems. You can achieve this by having a review process for all new and modified systems which involves both technical, security and operational staff.	This would be managed via the DPIA process at the beginning of each new project with approval provided by the Directors.	Compliant	
B8.3 Approved Software Are all computers and servers provisioned only with approved software from a list of authorised applications that you maintain? Explain how you achieve this. You should maintain a list of software that is used within the organisation and ensure that only software from this approved list is installed on your devices. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.	Yes – Standard software build is created for staff. Ongoing reviews of software in use are conducted and if surplus software is installed, this is removed. Staff do not have Admin access to their device so this should not occur. For cloud based SaaS, purchasing of software has to be authorized by one of the Directors, This is enforced through the InfoSec & Privacy and appropriate HR policies.	Compliant	

Question	Answer	Score	Comments
B8.4 Change Control Are changes to information systems, applications or networks reviewed and approved, and are users disallowed from making changes without approval? Describe the approval process. Changes to systems should be approved by a suitable person with a decision-making role in the business. Users should not be able to make changes without approval. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.	Yes – this is managed by the IT team in conjunction with the Director, Stephen Hackney. Changes to the development environment are managed by the development team which go through a testing process and have to be approved by the Directors.	Compliant	
B8.5 Network Security Controls Where identified as necessary in your risk assessment, have you identified and segregated critical business systems and applied appropriate network security controls to them? Explain how this has been achieved. If you run important business systems such as web servers containing client information, you may decide to segregate them from your main network in order to provide security.	All business systems are cloud based with appropriate access management in place. IT Manager oversees the system and has full control of the environment.	Compliant	
B8.6 Wireless Networks When you deploy wireless and wired networks, do you ensure that access is restricted only to authorised users? If you use wireless networks, you must ensure that wireless security (such as WPA2) is enabled so that only authorised devices are able to access your network. If you use a wired network, you must at a minimum ensure that access to network sockets is only provided in locations you control or use network access control technology.	Yes Applicant Notes: A separate network is in place for the team who are onsite at Changing Education. Access is available to staff only,	Compliant	
B8.7 Block and Monitor Do you use firewalls or other technology to block and monitor access to malicious internet locations/domains at the boundary of your networks? You could use a filtered DNS service such as (Quad9 or OpenDNS) or a firewall with rules blocking access to a list of suspicious URLs to achieve this.	Yes Applicant Notes: Firewalls are in place	Compliant	

Question	Answer	Score	Comments
B8.8 DPIA Do you ensure that a Data Protection Impact Assessment (DPIA) is carried out for new systems and projects? New systems and projects can present additional risks to the rights of data subjects. A DPIA can help highlight those risks and lead to an action plan for addressing them.	Yes Applicant Notes: No new systems have been introduced however the existing DPIA is scheduled for an annual review. This is performed in conjunction with an external consultant	Compliant	
B8.9 DPIA Remaining Risks If, after assessing all the risks in the DPIA, there is a high level risk left do you have processes for reporting this to your country's data protection office? Any significant risks that remain after the DPIA should be notified to your country's data protection office (ICO in the UK, Data Protection Commission in the Republic of Ireland).	Yes Applicant Notes: An extrnal consultant would be engaged to support the DPIA process. If all the risks identified were high following mitigation the project would not proceed.	Compliant	
B8.10 Supplier Security Procedures How do you ensure that all your suppliers (including cloud providers and sub-contractors) follow information security procedures that are certified to be the same as, or more comprehensive than, the information security procedures followed by your own organisation for the data involved in that contract? An example of such certification would be an independent audit of the whole business to ISO27001, the IASME Governance standard or Cyber Essentials. Bear in mind that a contract involving purely public data (such as hosting a simple website) may require a lower standard of information security that one involving more sensitive information (such as customer personal data).	Suppliers are reviewed to ensure that they meet or exceed the levels of security in place eg. CE, CE+, ISO27001. Where this is not evident on their website, a separate supplier questionnaire is issued. The organisation has a very small supplier base eg. Google etc. together with accountant, HR partner and aims to reduce risk with a smaller base	Compliant	
B8.11 Data Processing Agreements Do you have Data Processing Agreements in place with all suppliers that process personal data on your behalf? Such agreements set out the requirements for data security for a supplier and ensure that these requirements are clear.	Yes	Compliant	

Question	Answer	Score	Comments
A7.1 Account Creation Are users only provided with user accounts after a process has been followed to approve their creation? Describe the process. You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business.	Yes – all new starters have to be approved by the Directors, together with details of their role and access requirements	Compliant	
A7.2 Unique Login Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password? You must ensure that no devices can be accessed without entering a username and password. Users cannot share accounts.	Yes Applicant Notes: Yes – Devices cannot be shared. This is reinforced through regular auditing of the devices and through the InfoSec Policy	Compliant	
A7.3 Leavers Account Management How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation? When an individual leaves your organisation you need to stop them accessing any of your systems.	This is managed via the IT team who review all accesses and suspend through 1Password prior to deleting all accounts. Depending on the role, the individual may be placed on garden leave and will not therefore work their notice. In these instances, access is removed immediately.	Compliant	
A7.4 Staff Privileges Do you ensure that staff only have the privileges that they need to do their current job? How do you do this? When a staff member changes job role you may also need to change their access privileges to systems and data.	Only the IT team have Admin access to the devices. Access is managed based on role eg. Developers will have a different requirement to the Sales & Marketing teams. This is managed centrally via the IT Team and reviewed by the Director. Due to the size of the team, is it unlikely that individuals will change role within the business.	Compliant	

Question	Answer	Score	Comments
A7.5 Administrator Process Do you have a formal process for giving someone access to systems at an “administrator” level? Describe the process. You must have a formal, written-down process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.	Yes – this is restricted to just the Director (Stephen Hackney) and the IT Manager (Jamie Sutherland). If a user required admin access, access would be managed centrally with the password amended in 1Password after the system change had been completed	Compliant	
A7.6 Use of Accounts How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)? You must ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware.	Policy and training. Only two users have access to the Admin accounts- the Managing Director and the IT Manager. Strong passwords and 2FA are in place	Compliant	
A7.7 Managing Usage How do you ensure that administrator accounts are not used for accessing email or web browsing? You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.	Admin access is used by the Director and IT Manager who would not access the internet when making a change where Admin is needed.	Compliant	
A7.8 Account Tracking Do you formally track which users have administrator accounts in your organisation? You must track by means of list or formal record all people that have been granted administrator accounts.	Yes Applicant Notes: Yes – restricted to IT Manager and Director only.	Compliant	

Question	Answer	Score	Comments
A7.9 Access Review Do you review who should have administrative access on a regular basis? You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.	Yes Applicant Notes: Access is to IT Manager and Director only	Compliant	
A7.10 Two-factor Authentication Have you enabled two-factor authentication for access to all administrative accounts? If your systems supports two factor authentication (where you receive a text message, a one-time code, use a finger-print reader or facial recognition in addition to a password), then you must enable this for administrator accounts.	Yes	Compliant	
A8.1 Malware Protection Are all of your computers, laptops, tablets and mobile phones protected from malware by either: A - having anti-malware software installed, B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or C - application sandboxing (i.e. by using a virtual machine)? Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B.	A - Anti-Malware Software Applicant Notes: A – Windows Defender is in use.	Compliant	

Question	Answer	Score	Comments
A8.2 Update Daily (A) Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access? This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-virus software. You can use any commonly used anti-virus product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose.	Yes Applicant Notes: Windows Defender is in place	Compliant	
A8.3 Scan Web Pages (A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites? Your anti-virus software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.	Yes Applicant Notes: Windows Defender is in place	Compliant	
B9.1 Vulnerability Scan When was the last time you had a vulnerability scan on your system? You should carry out a regular vulnerability scan of your systems and network. Common tools which are free or low cost for SMEs such as OpenVAS, MBSA or Qualys can be used for this task. Many IASME CBs also offer this service.	Security Essentials scans the machines every week. No manual checks.	Compliant	
B9.2 Penetration Test Where identified as necessary in your risk assessment, when was the last time you had a penetration test carried out on your critical business systems? Where you have high risk systems, such as a web server with customer information, you should carry out penetration tests to ensure that the system is secure from external attackers. Penetration tests are often carried out after major system upgrades or changes.	Not required but is scheduled to be conducted during Q4 for the app and Connect Systems	Compliant	

Question	Answer	Score	Comments
B9.3 Improve Security How did you act to improve the security of your system on the basis of the scan results?	Depending on severity, any areas for improvement identified in the scan will be implemented	Compliant	
B10.1 Review Event Logs Does the organisation review event logs (including alerts and errors) at least weekly? If you use an automated system to monitor events and flag up suspicious activity, then that is acceptable and you should answer yes to this question.	Yes Applicant Notes: Review of the Connect logs is performed by the development team. Reviews of Google logs is performed by the IT Manager	Compliant	
B10.2 Audit Trail Is an audit trail of system access and/or data use by staff maintained in a central location for all relevant systems and reviewed on a regular basis? Describe how you achieve this. You should ensure that logs of system access and use are pulled to a central location. This could be using a cloud-based solution or a local server.	Yes – this is managed by the IT Manager	Compliant	
B10.3 Time Synchronisation Do you ensure all you devices have their time set accurately to ensure logs and audit trails are in sync with each other? You can make sure your devices are synchronised by changing the date/time preferences to enable automatic or internet time.	Yes Applicant Notes: Devices are set to enable automatic time	Compliant	
B10.4 Log Security Do you ensure that any event logs and audit trails are kept secure and do not expose sensitive information to unauthorised users? You should ensure that any logs are stored in a safe location and that error messages do not return sensitive information to external or internal users.	Yes Applicant Notes: Logs are maintained with AWS and can only be accessed by developers.	Compliant	

Question	Answer	Score	Comments
B11.1 Regular Backups Are data stored on the business premises backed up regularly (at least weekly) and restores tested at appropriate intervals (at least monthly)? You must ensure a copy of all important data is made regularly and stored in a location other than your main place of business. Some organisations will use a cloud backup whereas others will rely on the use of encrypted USB drives or tape drives. You must also regularly try to access the copy of the data to ensure that it is valid and that you would be able to access it if needed. You don't need to restore the whole data set, just a selection of files to ensure accessibility - this process could be automated.	Yes Applicant Notes: Data is stored and maintained within the AWS environment, with version in control for data bases.. 90 days of email are retained.	Compliant	
B11.2 Backup Protection How do you ensure all backups are secured with an appropriate level of protection for the type of data they contain? Your backups contain your sensitive company data and must be protected with the same amount of effort as the main location of the data. Backups should be stored securely and encrypted.	Users told not to store information on their local machines in order to ensure that all data is appropriately backed up and maintained. Cloud providers are used	Compliant	
B11.3 Backup Location Is a backup copy held in a different physical location? You must keep at least one backup copy in a different physical location from your main office. If the main office was destroyed by fire, you would still be able to access the backup copy if it is in a different location.	Yes Applicant Notes: cloud backups are used	Compliant	

Question	Answer	Score	Comments
B12.1 Incidents Reported/Recorded Are all information security incidents or suspected weaknesses reported and recorded, and do you provide a method for all employees and contractors to report security incidents without risk of recrimination (or anonymously)? You must provide a route for staff and contractors to report any security weaknesses they encounter - including staff acting incorrectly and configuration issues. It is important that staff can do this either anonymously or in a way that makes it clear there is no risk of negative consequences to them for highlighting an issue.	Yes Applicant Notes: An incident management process is in place which asks that users report all incidents. Culture is open and encourages transparency.	Compliant	
B12.2 Unauthorised Installation Are users who install software or other active code on the organisation's systems without permission subject to disciplinary action? Users who take risks and install software without permission must be subject to your disciplinary procedure.	Yes Applicant Notes: Malicious or deliberate breach of policies will be treated as gross misconduct. This is linked to the disciplinary process.	Compliant	
B12.3 Formal Investigation Do you formally investigate information security incidents to establish their cause and their impact with a view to avoiding similar events? You must investigate incidents using a team of knowledgeable and appropriately skilled people to ensure that changes are made to prevent the incident reoccurring. You can use an external company to provide this service to you if needed.	Yes Applicant Notes: No incidents have occurred to date that would warrant an investigation. Internal investigation would take place in the first instance with external support requested where appropriate	Compliant	
B12.4 Forensic Examination If required as a result of an incident, is data isolated to facilitate forensic examination? How is this done? Forensic examination of data can help identify the cause of an incident. You can use an external company to provide this service to you if needed.	Logs would be copied to a secure area. If appropriate, litigation hold would also be implemented on emails	Compliant	

Question	Answer	Score	Comments
B12.5 Report Incidents Do you report incidents to external bodies as required, such as law enforcement for criminal activity and the relevant authorities (such as the UK ICO) for personal data breaches? You should report incidents to law enforcement for investigation where appropriate. You may also be required to report personal data breaches to your country's data protection office.	An incident management and reporting process is in place. External consultancy support would also be sought	Compliant	
B12.6 Records Kept Is a record kept of the outcome of all security incident investigations to ensure all lessons have been learned from each event? The result of any investigations should be recorded so that trends can be identified over time and to aid future investigations.	Yes Applicant Notes: A breach register is in place to track with lessons recorded for each event. The register encourages the identification of any root cause trends eg. where education where may be required etc,.	Compliant	
B12.7 Clear Roles Do all staff involved with incident management have clear roles and responsibilities and have they all received appropriate training? It is important that staff involved in investigating incidents have the knowledge and skills required so that their involvement assists and does not worsen the impact of any incidents.	Yes Applicant Notes: Incident investigation would be managed by the Data Manager who has good knowledge of the systems in use across the organisation. Appropriate authority is in place to ensure that any actions from the incidents can be managed through to closure.	Compliant	
B12.8 Incident Response Test Do you test your incident response process at least once per year? You should carry out a table-top exercise where you create a plausible scenario (such as a staff member accidentally emailing data to a client) and run through the incident response process to confirm that it works for your organisation. You can also treat any real incident as a test of the process.	Yes Applicant Notes: Response has been tested with a 'live' event earlier in the year. A documented process is in place. Recommendation that 'Exercise in a Box' is also incorporated into incident planning.	Compliant	

Question	Answer	Score	Comments
B13.1 Produce Plan Do you ensure that business impact assessments, business continuity and disaster recovery plans are produced for your critical information, applications, systems and networks? A business impact assessment assesses the risk of a critical function being disrupted and outlines the actions to be taken to restore the function.	Yes Applicant Notes: A business continuity plan is in place that has reviewed a number of key areas - people, processes, property and key partners.	Compliant	
B13.2 Review Plans Do you review the business continuity and disaster recovery plans at least once per year? Who is involved in the review? You should involve a group of people from across the organisation to review the plans including representation from the board/director/partner/trustee level.	This will be reviewed annually as part of the IASME process with the Directors of the organisation	Compliant	
B13.3 Test Plans Do you test the business continuity and disaster recovery plans at least once per year by running a simulation exercise that includes cyber incidents? You should test your plans by at least running a table-top exercise each year where you test how the plans would operate in major incident. Your risk assessment may indicate that you need to carry out such tests more often.	Yes Applicant Notes: A 'live' simulation has been run following the lockdown in March 2020 which moved all employees from being based in the office to working remotely,	Compliant	
A3.1 Head Office Is your head office domiciled in the UK and is your gross annual turnover less than £20m? This question relates to the eligibility of your company for the included cyber insurance.	Yes	Compliant	

Question	Answer	Score	Comments
A3.2 Cyber Insurance If you have answered 'yes' to the last question then your company is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here. The cost of this is included in the assessment package and you can see more about it at https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/.	Opt-In	Compliant	
A3.3 Total Gross Revenue What is your total gross revenue? Please provide figure to the nearest £100K. You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification. Please be as accurate as possible - figure should be to the nearest £100K	£650K	Compliant	
A3.4 FCA Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.	No	Compliant	
A3.5 Domiciled Operation Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.	No	Compliant	

Question	Answer	Score	Comments
A3.6 Email Contact What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.	s.hackney@changingeducation.co.uk	Compliant	
All Answers Approved Have all the answers provided in this assessment been approved at Board level or equivalent?	Yes	Compliant	
Cyber Declaration Signed Has the attached Cyber Declaration been downloaded (by clicking here), completed and signed (by a Board level or equivalent signatory), then uploaded (using the function provided below)? Please note: The file upload must be in .PDF, .JPG or .PNG format and a maximum file size of 5MB. If your file is larger than 5MB, please contact info@iasme.co.uk.	Yes	Compliant	

CYBER ESSENTIALS

CERTIFICATE OF ASSURANCE

Changing Education Group

67 Kingsleigh Road, , Stockport, , SK4 3PP

COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS SCHEME

NAME OF ASSESSOR : Chris Chan

CERTIFICATE NUMBER : IASME-CE-013166

PROFILE VERSION : April 2020

SCOPE : Whole Company

DATE OF CERTIFICATION : 2021-02-16

RECERTIFICATION DUE : 2022-02-16

CERTIFICATION MARK

CERTIFICATION BODY

CYBER ESSENTIALS PARTNER

CYBER ESSENTIALS CERTIFIED

CS RISK Management part of Moore Kingston Smith

IASME CONSORTIUM

The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.

IASME CONSORTIUM

GDPR CERTIFIED

CERTIFICATE OF ASSURANCE

VERIFIED SELF-ASSESSMENT

Changing Education Group

67 Kingsleigh Road,
Stockport,
SK4 3PP

SCOPE : Whole Company

COMPLIES WITH THE IASME GOVERNANCE STANDARD
THIS CERTIFICATE IS VALID UNTIL 2022-2-16 AND IS SUBJECT TO
CONTINUOUS SELF ASSESSMENT AND INDEPENDENT ANNUAL REVIEW

DR EMMA PHILPOTT MBE
CEO

DATE: 2021-2-16

CERTIFICATE NUMBER: IASME-SA-000646

The IASME Consortium Limited, Registered Office:
Wyche Innovation Centre, Walwyn Road, Malvern,
Worcestershire WR13 6PL

IASME Consortium ®

SUTCLIFFE & CO.
INSURANCE BROKERS

Evidence of Insurance

Eligible Cyber Essentials Certificate Holders

Master Policy Number	**CY0396599**	
Master policy in the name of	**Holders of current Cyber Essentials Certificates**	
Cyber Essentials Certificate No.	13166	
Insured Name	Changing Education Group	
Insured's Address	67 Kingsleigh Road, Stockport, SK4 3PP	
Turnover	Up to £20,000,000	
Period of Insurance	From: 2021-02-16 To: 2022-02-16 Both days at 00:01 a.m.	
Insurer	XL Catlin Insurance Company UK Ltd	
Wording	Angel Cyber Essentials Liability insurance CYB 12/20 ANG.3	
Cyber Liability	Limit of Liability	£25,000 in the Aggregate (including defence costs and expenses)
	Excess	£1,000 per claim other than; £5,000 in respect of any loss form any claim emanating from activities in the USA or Canada
	BI Excess	6 hours
	Jurisdiction	UK & Crown Dependencies
	Geographical Limits	Worldwide
Retroactive Date	Inception date of the first cyber policy issued by Angel or Cyber Essentials Evidence of Insurance issued to the Insured. The retroactive date will be maintained at renewal providing there is no more than a 14 day gap from the end of the expiring Cyber Essentials certificate to the start of the renewing Cyber Essentials certificate.	

At first suspicion of an incident the organisation should immediately contact the **Accenture Response Hotline on 0800 085 9483.**

For Insurance questions please contact enquiries@sutcliffeinsurance.co.uk or call 01905 21681.