DSPT information to assist care providers

Company name	My Learning Cloud
Product name	Lumis Learning Environments

DSPT	Approaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
1.2.1	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber security Confirm that your organisation has a policy or policies in place to cover: Data Protection, Data Quality, Record Keeping, Data security and, where relevant, network security.	Does your data processing agreement impact the care provider, if so please document your policy and the scope where it would affect the customer	Internally, yes we do. All these policies are part of our ISO27001 Internet Security framework.
1.4.1	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Please explain how your product manages and shares personal information	Internally, yes. We don't hold any personal or sensitive information on our application.
1.6.1	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Please explain how your product keeps personal data secure	N/A see above
1.6.4	Yes	What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately? Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.	Discuss with care providers the arrangements they should consider to minimise the risks if mobile phones are lost or stolen and offer advise as necessary.	Internally we have PINS on work mobiles, with 2 factor authentication and strong passwords for email access. If a phone is lost its reported to IT and is remote wiped using Mobile Iron mobile device management software
1.6.5	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data? This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO	Care providers complete their own DPIAs, however may wish to discuss the supplier DPIA relevant to the technology that they are implementing to determine items such as data flows and data transfers.	My Learning Cloud has a DPIA in place.
1.6.6	No	If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Does your product have any tools to manage BYOD devices? If so please document how this helps a customer	No we do not have a BYOD policy. Staff are discouraged from using their own devices.
1.7.4	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Please document your data retention criteria	**In terms of Customer data and information**, yes we do we have different lengths for customer contracts and data
1.8.3		What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	Please give the reverse of the question, explained what they have implemented to mitigate risks, so the customer can rank them for all systems in use by them	a) The biggest risk is disclosure of authentication credentials via phishing attack b) Another big risk is our customer server being hacked . Our mitigation against our biggest risk is that we run quarterly phishing tests and we provide cyber security e learning training for all staff. For the Server quarterly patching and quarterly PEN tests are conducted to look for vulnerabilities.
4.1.2	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Please document how your product provides access control and audit of this information	We don't carry any personal and confidential data in our application.
4.2.5	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	If your product can assist in managing access rights then please explain here	its audited through the Server and on other third party products like Atlassian and whenever any individual leaves a customer database, the individual is removed from all databases. Internally - our HR system notifies IT of any changes of any starters leavers or changes so that the IT department can update accordingly.

DSPT information to assist care providers

Company name	My Learning Cloud
Product name	Lumis Learning Environments

DSPT	Approaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
4.5.4	Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice? If your organisation has any It systems or computers it should provide advice for setting and managing passwords. Each person should have their .own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be "strong" i.e. hard to guess.	If your product can assist in managing password practice then please explain here	**In terms of Customer data and information**, My Learning Cloud enforce strong passwords on all of our systems and **In terms of internally** we use strong passwords with additional 2 factor authentication for all access points.
6.1.5	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	Does your product have any tools to give visibility of who has accessed each individual data record?	In terms of internally If we had a breech we have policies and procedures in place that are in line with ICO best practice.
6.2.3	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date? This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions.	If you provide any of these devices then please explain any malware management included on them.	Yes we have centrally managed anti virus and anti malware protection that is kept up to date. We use MacAfee and E Policy orchestrator version 5.1 that is our management tool that is used to deploy MacAfee End Point protection Suite of programs.
7.1.2	No	Does your organisation have a business continuity plan that covers data and cyber security?	Please explain your business continuity plans for data and cyber security here.	Yes My Learning Cloud has a Business Continuity Plan in place that covers data and cyber security
7.3.1	Yes	How does your organisation make sure that there are working backups of all important data and information? It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's back up systems work and how you have tested them.	Please document your data backup process.	**In terms of Customer data and information,** an annually dry run is scheduled of the disaster recovery process, backups are taken hourly which are stored for 24 hours and daily backups are stored for 6 months. Backups are stored on a secure remote servicer that is capable of restoring system functionality should the primary server go down. In terms of Internal data, backups are tested on a regular basis - weekly monthly and quarterly. They are tested by doing recoveries and of individual files, folders and complete servers.
7.3.4	No	Are backups routinely tested to make sure that data and information can be restored?	Please document your data backup process.	**In terms of Customer data and information** backups are routinely tested, this is part of the dry run. In terms of internal date, yes.
8.3.5	Yes	How does your organisation make sure that the latest software updates are downloaded and installed It is important that your organisation's IT system (s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question.	Does your product have automated updates. If so, please document how this occurs, and how a customer can check which version they are running.	In terms of Customer data and information we do computer updates and we do server patching that happens daily automatically. **In terms of internally** we use a Microsoft product called Windows Server Update Services which deploys security patches and updates to all devices. Standard software updates happen overnight automatically and the customer server is updated quarterly or asap if critical vulnerability discovered
9.1.1	No	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Do you manage any WIFI routers for customers? If so, please explain how.	Yes - and No we don't manage any WIFI routers for customers

DSPT information to assist care providers

Company name	My Learning Cloud
Product name	Lumis Learning Environments

DSPT	Approaching	DSPT Question	Supplier information (CASPA)	Responses (only complete where relevant)
9.6.2	No	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted? Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people)	Cloud systems are designed to reduce the need to hold any data locally, using API's to directly connect cloud based analysis and document system without the need to expose data to local storage risks. However, where the supplier includes provision of removable devices, these should be appropriately protected using encryption and /other technical measures.	All laptops and devices are encrypted whether they hold personal data or not,
10.1.2	No	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Please give contact details here for the provider to include in their supplier list	Yes
10.2.1	Yes	Do your organisation's IT system suppliers have cyber security certification Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace	Please confirm if you have cyber security certification	All our third party software suppliers that we use adhere to cyber security certification including but not limited to the following : AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 and CSA STAR CCM v3.0.1. . Aptum have All Data Center Operations are ISO 27001 certified and our managed services are audited against SOC 1 and 2 Type II framework.Internally My Learning Cloud hold ISO 27001 and Cyber Essentials Plus
		Has your organisation completed the DSPT?	Have you completed the DSPT , if so where do you display this ?	YES
		GDPR statement and contract with supplier	Please give a link to your GDPR statement, ideally in as plain English/easy to understand format as possible	Yes it is on our website and here is the link : https://www.mylearningcloud.org.uk/privacy-policy