CHUBB

Standard Cover		
Section	**Standard Limit of Indemnity**	**Standard Deductible**
Privacy Liability	100% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Network Security Liability	100% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Media Liability	100% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Incident Response Expenses	100% of Limit of Indemnity	Nil

Optional Covers – Can be purchased for additional premium		
Section	**Standard Limit of Indemnity**	**Standard Deductible**
Cyber extortion	100% of Limit of Indemnity Can be purchased as bundle with Data Asset Loss & Business Interruption	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Data asset loss	100% of Limit of Indemnity Can be purchased as bundle with Cyber Extortion & Business Interruption	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Business interruption	100% of Limit of Indemnity Can be purchased as bundle with Data Asset Loss & Cyber Extortion	12 hours
Recovery costs	100% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover

---

Standard Sub-limits applicable		
Consumer redress fund	50% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Payment card loss	50% of Limit of Indemnity *must be PCI Compliant*	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover
Regulatory fines	50% of Limit of Indemnity	£1,000 up to £2.5m turnover/ £2,500 up to £10m turnover

Jurisdiction	Worldwide excluding USA / Canada
Territory	Worldwide excluding USA / Canada
Retroactive date	Inception unless Cyber Insurance purchased previously

Additional terms, conditions, exclusions, and endorsements:

Section	Description
Endorsement	Chubb Incident Response Endorsement – Standard
Subjectivities	Satisfactory, signed and dated Chubb ERM Underwriting Statement of Fact

Chubb ERM Underwriting Statement of Fact for Elementary and Secondary Schools/Academies (Schools Advisory Service)

Qualifying Questions		Yes	No
1	Do you the Insured have an up to date antivirus & malware protection in place on all systems & connected devices? ***If 'No', Please see page below for any mitigating controls the insured has in place***	☐	☐
2	Do you the Insured have back up for all mission critical systems and files (to a secondary storage environment at least monthly) ***If 'No' - Please provide information for compensating controls below***	☐	☐
3	Do you the Insured implement access control or password protection policies for your network and critical systems? ***If 'No', Please see below for any mitigating controls you the insured has in place***	☐	☐
4	Do you the Insured, or your outsourced service provider, accept payment card transactions? ***If Yes - Are they compliant to the level of PCI that applies to their company?***	☐ ☐	☐ ☐
5	Within the last 3 years, have you the Insured had any cyber incidents; known cyber events or become aware of any matter that could lead to a claim under a cyber insurance policy? ***If 'Yes', was this a one-off incident that did not result in any financial impact to the organisation (please provide further information if 'No')***	☐ ☐	☐ ☐
6	Do you the Insured have a fully implemented staff training program in place for data & privacy protection? ***If 'No', please provide information below on how employees are trained or made aware of basic security practices and their role in keeping sensitive information safe***	☐	☐

7 Who do you use as your main software and/or network platform where an outage of it would impact on capability to operate fully?

_____

_____

_____

I/we declare that I/we have made a fair presentation of the risk, by disclosing all material matters which I/we know or ought to know or, failing that, by giving the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances.

Signatory Name and surname

Function

Date

Signature

Further info to support Qualifying Questions:

Q1 – Answered 'No', but have following mitigating controls (Please circle):

Existence of intrusion detection and prevention

Active updating anti-virus signatures

Use of Monitor Logs

Receipt and Action of Vulnerability Alerts

Firewall in place to mitigate Front End attacks

NONE OF THE ABOVE – please provide further info

Q2 – Answered 'No', but please provide information for compensating controls in place to address this:

Q3 – Answered 'No', but have the following mitigation controls (Please circle):

Existence of intrusion detection and prevention for critical systems

Use of Monitor Logs

Authorisation Procedure in place for User Access to critical systems

User Access Termination Procedures

Periodic Password Updates

NONE OF THE ABOVE – please provide further info

Q5 – Details of incident, event, claim (including financial impact to business):

Q6 – Answered 'No', please provide information below on how employees are trained or made aware of basic security practices and their role in keeping sensitive information safe:

Helpful Definitions:

Q1 - 'Connected Devices' - electronic device that is connected to a network, such as laptops, notebooks or tablet computers.

Q2 - 'Files' (collection of data &/or information)

Q2 – 'Secondary storage environment' (devices and media that are not constantly accessible by a computer system)

Q3 - 'Access control' - Ensuring only those who should have access to systems to only have access and at the appropriate level.

Q3 - 'Password protection' - Allows only those with an authorised password to gain access to certain information.

Q4 - The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle branded credit cards from the major card schemes. Please view https://www.pcisecuritystandards.org/faqs for full information.