Partner/Vendor Request for Information – Privacy, Data Protection and Security

Third Party Contact Information		Suggested responses
1	Company name:	NetSupport Software Group
2	Location of Head Office:	NetSupport House, Towngate East, Market Deeping, Peterborough, PE6 8NE, United Kingdom
3	Account manager / Contact name:	**Please contact the Sales team for details of your account management**
4	Account manager / Contact phone number:	
5	Account manager email address:	
6	Please describe the nature of the business relationship and activities.	Provider of cloud-hosted solution for classroom and lesson management and learning tools, safeguarding, and device management.
Data Protection Representative		
7	Data Protection Contact name:	Helen Hankinson
8	Data Protection Contact email address:	support@netsupportsoftware.com
9	Data Protection Contact phone number:	+44(0)1778 382272
Certifications and Standards		
10	ISO 27001 Information Security	uncertified
11	ISO 9001 Quality Management	uncertified
12	ISO 22301 Business Continuity	uncertified
13	ISO 20001 Service Management	uncertified
14	PCI DSS	uncertified
15	Cyber Essentials/Cyber Essentials Plus	uncertified

Data Protection Compliance (DPA/GDPR)		
16	Does your organisation operate in full compliance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA)? Including the following principles: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Security • Accountability	As a Data Processor, we operate under the instructions of the Data Controller as set out in the Data Processing Agreement: Data Processing Agreement | classroom.cloud We take every measure we can to support schools as they follow the 7 principles.

17	Do you consider your provision of services to fall within the scope of the Age-Appropriate Design Code? If so, please confirm that you are compliant with the requirements of the Code and provide any evidence of certification.	As the service is designed for use by a school as the Data Controller, classroom.cloud is not considered to be an Internet Society Service, and so would not be covered by the code. However, we have taken several steps to ensure that schools can be mindful of the privacy and rights of their learners, including setting time/day/date schedules when learner devices can be accessed for both the classroom tools and the safeguarding tools. We also provide a range of functions that schools can turn on as needed, to help learners be aware of when they are being viewed, are able to control whether teachers can connect and also whether they see the teacher's desktop when shared (functions may depend on device OS functionality).

18	What customer data do you process, store or transmit (if any)? e.g. documents, staff details, customer names, addresses, account numbers, PAN data, audit reports, system backups, contracts, service management records, source code, multimedia.	The platform is designed to be able to process the following groups of personal data: • Contact details • Information we get from other systems • Information that identifies users • Information on how your users use classroom.cloud • Lesson activities • Possible safeguarding issues (an optional feature) As a Data controller, you may use the platform to process additional groups of data. This is the choice of each school and should be appropriately recorded by the school.
19	Are you registered with the UK Information Commissioners Office (or equivalent)? If so, please provide details (registration number).	We are registered in the UK under the ICO's register of fee payers: **Z9139408.**
20	How is data transmitted to/from customers? Please detail the methods, volumes and frequencies.	Depending on the functionality being used, data is processed by an agent installed on the school/learner's device and then sent over a secure connection to our cloud-hosted servers. Depending on the functionality enabled, different volumes of traffic will be transmitted.
21	At what locations is customer data stored, transmitted or processed? Please also detail any restricted transfers.	The platform is hosted on Microsoft Azure on a regional basis (e.g. UK data in UK Azure hosting, US data in US Azure hosting). More details on the specifics of the this and other sub-processors can be found in the Data Processing Agreement.
22	Do you maintain 'Records of Processing' (GDPR Article 30) detailing at least the purpose of processing, categories of data subjects, categories of personal data, data retention and data-sharing activities?	To support schools with their Record of Processing Activities, we have set out the suggested purpose, categories and lawful basis within our Data Processing Agreement. It also covers the default retention within the portal. We do not share any of your data. Where integrations are enabled by schools, this allows us to transfer to, or process data from, other data processors you have agreements with. These options are also set out in the Data Processing Agreement.

23	Please describe your Data Retention Schedule and capabilities as they relate to customer personal information.	As set out in the Data Processing Agreement, we continue to hold all 'active' data (data that has been provided and is linked to active accounts on a verified licence) until the following: • If your subscription licence has run out and accounts are no longer active, personal data is kept for 30 days and then securely deleted. • We also operate a rolling backup that retains safeguarding data for 13 months. • We can extend the length of the rolling backup, but additional agreements and costs may be needed.
24	Approximately how many people have access (or could obtain access) to customer data (excluding customer employees)?	Information about sub-processors is available through the Data Processing Agreement. Access to customer data is carefully controlled and regulated within NetSupport. Development and Testing is done using dummy data and does not make any use of live data sets. Product Support may access customer data where this is sent from the customer.
External Parties		
25	Is data shared with, or processed by, any third parties or sub-processors? If so, please provide details.	No data is shared with third parties (as set out by the definition under EU/UK GDPR). All information about sub-processors is available through our Data Processing Agreement. Where integrations are enabled by schools, this allows us to transfer to, or process data from, other data processors you have agreements with. These options are also set out in the Data Processing Agreement.
26	If shared with third parties, how are compliance with data protection obligations and the security of data maintained?	No customer data is shared with third parties (as set out by the definition under EU/UK GDPR).
27	Are processing agreements and NDAs in place with all sub-processors or third	Clear contracts are in place with all sub-processors that meet or exceed the requirements within the Data Processing Agreement.

	parties that may have access to sensitive information and/or intellectual property?	
Policies, Processes and Procedures		
28	Does the organisation operate any Security Policies? E.g. Information Security Policy, Acceptable Use Policy. If so, please list or describe.	We operate a range of practices across the following policies: 1. Acceptable Use Policy 2. Security Awareness Policy 3. Information Security Policy 4. Disaster Recovery & Business Continuity Plan 5. Change Management 6. Incident Response Policy 7. Remote Access Policy 8. Bring Your Own Device Policy 9. Media Destruction, Backup and Retention Policy 10. Data Classification Policy. Company policies are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.
29	Does the organisation have documented agreement and commitment to information security from top management?	Information Security is under the responsibility of a Director of the Board, Andy Gibbons, and is a core aspect of operations management. It is supported by a team including a certified Data Protection/Privacy specialist.
30	Is there a mechanism established to ensure employees have read and agreed to security policies applicable to them?	As part of induction, all staff have to agree to the company's policy on the use of computers, personal data and customer information, with specific instructions given to staff dependent on their roles within the organisation.
HR Controls		
31	Are all employees subject to security awareness training? At what point and frequency are employees provided with such training?	Information is readily available to all staff on information security and data protection, and is a regular feature in communications and newsletters.

32	Has the organisation appointed one or more resources to be responsible for information security? If so, please provide roles and responsibilities.	The Owner for Information Security is Andy Gibbons, Technical Director, supported by Helen Hankinson (DPO and Central Admin) and Tony Sheppard CIPP/E (Technical Consultant and Pre-Sales).
33	Are new employees subject to background checks prior to employment? If so, please detail what checks are undertaken, e.g. CRB/DBS.	Staff employment history and references are reviewed for non-sensitive roles, and trusted individuals appointed to roles where elevated access is subsequently needed, with review of requirements on the job roles by Directors when required.
Risk Management		
34	Is a risk assessment conducted at a frequency of no less than once per year?	Risk assessments are part of an ongoing programme and not limited to once a year.
35	Are individual information security risks recorded using a risk register?	A central risk register is used to maintain records on all security risks, and subsequent treatment. Company policies are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.
36	Are identified risks measured, prioritised and remediated using a risk treatment plan?	Risk management is a core activity, and any risks identified are rolled into our ongoing development process and prioritised accordingly. Treatment plans are signed off at board level.
Incident Management		
37	Have you had any security incidents within the last year? (e.g. crime, fraud, attempted fraud, breach of security policy, system intrusion). If so, please provide reports and supporting information.	No.
38	Do you have a notification process whereby customers and clients will be made aware of any relevant incidents (including data protection breaches)?	We notify impacted customers at the earliest opportunity. Company policies are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.
39	Do you have an established and documented methodology for identifying and responding to security incidents?	This information is within our Incident Management Policy.

		Company policies are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.
Physical Security		
40	Please detail physical security controls regarding access to facilities. For example: access cards, turnstiles, CCTV, intruder alarms.	Information on security for hosting is available from the Data Processing Agreement. NetSupport House also manages the physical security of the building via access control, security passes, CCTV and other organisational measures (visitor sign-in/chaperoning).
41	Are any sensitive areas subject to additional security or availability controls? If so, please provide details on such controls.	Information on security for hosting is available from the Data Processing Agreement. NetSupport House also manages the physical security of the building via access control, security passes, CCTV and other organisational measures (visitor sign-in/chaperoning).
42	Do you have a method of identifying visitors and recording visitor history to physical premises? Please describe.	Information on security for hosting is available from the Data Processing Agreement. NetSupport House also manages the physical security of the building via access control, security passes, CCTV and other organisational measures (visitor sign-in/chaperoning).
Network Security		
43	Do you have accurate and maintained network diagrams and documentation detailing endpoints, egress points and traffic flows?	Infrastructure design and documentation are complete and regularly updated as needed. These are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.
44	Are penetration testing exercises conducted at least every 6-12 months? If so, please provide details (provider, tools, scope).	Weekly and monthly penetration testing is completed across the corporate environment, including hosted services such as classroom.cloud. Development, Testing and Production are all separate environments, with no shared resources. No public and/or live data is used within Development or Testing.
45	Are controls in place to monitor and control internet and email access? E.g. spam filters and content filters. Please provide details.	Corporate devices are centrally managed, with full internet controls and monitoring. Email traffic uses Proofpoint. Within the classroom.cloud platform, notifications sent to assigned users are passed through a messaging service which securely prevents spoofing and relaying.

46	Are centrally-managed anti-virus and anti-malware controls deployed within the infrastructure? If so, please provide details.	As well as the available technologies from Microsoft Azure, the corporate environment is also protected through the centralised management of anti-virus and anti-malware through Avast.
47	Is there an established and practised patching strategy in place? If so, please provide details.	Infrastructure design and documentation are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality. Updates to infrastructure and services are also contained within the development and testing process to ensure consistent quality and security to the platform.
48	Do you have a method of identifying network security vulnerabilities? If so, please provide details.	Infrastructure design and documentation are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality. Several security plug-ins are in use across the company infrastructure, enabling prompt notification of any issues or updates to websites and services. Security measures are also in place for notification of secure logins to services as part of security tracking measures. All approaches are in line with processes set out to meet Cyber Essentials Plus (presently being recertified).
49	Is there an appropriate logging system in place to collect system and event logs from across the estate? Please provide details.	Infrastructure design and documentation are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality. Logs for a range of activities (logins, account controls, etc) are recorded and retained for a year. These are reviewed for security, bugs and reported issues on an ad-hoc or as-required basis.
Data Encryption		
50	If customer data traverses public or unprotected networks, is it protected by a strong encryption algorithm? If so, what encryption is used?	All data is transmitted using TLS (1.2 or 1.3). Additionally, sensitive data is end-to-end encrypted using AES Encryption.
51	Is customer data encrypted at rest (servers, databases, backups, etc.)? If so, what encryption algorithms are in use?	All data is encrypted at rest and more information can be found at Azure Data Encryption-at-Rest - Azure Security | Microsoft Docs (Disk encryption and SQL encryption). Local passwords are hashed with a salted hash and encrypted at rest. Where organisations use SSO for authentication, the password details are not stored within the database.

52	Through what interfaces does the organisation transfer business data? How are these adequately secured?	The agent transmits and receives data across an encrypted connection with the platform, as covered in Q 50.
53	Are employee laptops encrypted? If so, please describe these controls.	No customer data should be held on staff laptops. All staff laptops use hardware disk encryption (BitLocker and File Vault) and are centrally managed.
Access Control		
54	Are access levels granted according to principle of least privilege?	Privileged Identity Management is in place to ensure that access is elevated when needed and subsequently reduced when not in use (https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure). This is controlled centrally, but we also operate on a basis of least privilege for all users.
55	Are access levels reviewed on a regular basis? If so, at what frequency?	Access levels are reviewed on a needs basis, including as job roles change and for starters/leavers.
56	Are user accounts attributable to uniquely identifiable individuals to ensure accountability and non-disruptive revocation of access, i.e. no shared accounts? Please detail any exceptions and compensating controls.	All accounts are uniquely assigned and used. Additional operational processes are used to ensure that access is elevated when needed and subsequently reduced when not in use. Any shared/master account is secured and not used save as part of Business Continuity and Disaster Recovery.
57	Are password criteria for networks, operating systems and applications sufficiently complex? (Please describe).	All network and application passwords comply with the complexity requirements as defined in the Information Security Policy, in addition to this where possible all authentication is configured to use Multi-Factor Authentication.
Business Continuity		
58	Do you have a Business Continuity plan? If so, please provide details and supporting evidence.	We operate a range of practices across the following policies: 4-Disaster Recovery & Business Continuity Plan Company policies are held as commercially sensitive and/or privileged information and are not shared externally as part of our approach to security and confidentiality.

59	Are Business Continuity and Disaster Recovery plans tested on a regular basis? If so, please provide details and supporting evidence.	Partial DR tests are performed monthly with a full DR test annually. Tests are a combination of walkthroughs, simulations and full-interruption testing.
60	Are backup and restore procedures tested on a regular basis? At what frequency, and to what extent does this occur?	Automated backup and recovery tests are performed daily, and supervised tests weekly. A full system restore is tested monthly as part of the DR partial test.
61	What is the Recovery Point Objective and Recovery Time Objective for disaster recovery (if available)?	The RPO varies for the different systems and services that are covered by the Disaster Recovery plan. The maximum RPO for any system is 24 hours. As with the RPO, the RTO also varies depending on the system or service. The maximum RTO for any service or system covered by the disaster recovery plan is 24 hours.
Software Development (if applicable)		
62	Are development processes and practices defined and documented, including security consideration and best practices?	Development practices operate using development environments with embedded security and best practice features, ensuring that the widest range of coverage is provided for all security needs.
63	Are software developers trained in secure coding methods and practices? If so, please provide details.	The Development team is selected based on their ability to code using appropriate technologies, and to maintain and update their knowledge in their areas of expertise.
64	Are internally developed applications (including web applications) subject to penetration testing at least once per year?	All web services, including the classroom.cloud website, are tested on a weekly basis, with full review by the infrastructure group, with appropriate treatment plans developed and agreed. Additional tests are undertaken on an ad-hoc or as-required basis.
65	Are Development and Testing environments adequately separated from live/production environments and data? Please provide details.	Development, Testing and Production environments are separate and segregated. No live data is used within Development or Testing.
66	Where applicable, does your product support Single-Sign-On (e.g. SAML) to integrate with customer systems user credentials.	classroom.cloud will integrate with Microsoft 365, Google Workspace for Education and ClassLink.

We appreciate your time in responding to this Request for Information.

Completed by	Tony Sheppard CIPP/E
Position	Pre Sales Consultant
Authorised by	Andy Gibbons
Position	Technical Director
Date	23/11/2021

Acknowledgements

This template is prepared by Tony Sheppard (My Data Protection World).

Original design and contribution by Elliott Lewis (ParentPay) as part of the Education Data Matters group (https://www.educationdatamatters.org.uk).

Additional contributions by Alexander Banthien (GDPRiS), Claire Archibald (Education Data Hub, Derbyshire County Council) and Jessica Sweet (Coventry City Council).

Peer review and contributions by the DPOaaS Slack Group Community.

This is version 1.3 – 23rd November 2021.