Schoolcomms Security and Data Protection RFI (Request for Information)

This document should be considered Confidential throughout it's lifecycle.

Third Party Contact Information		
1	Company name:	Schoolcomms
2	Location of Head Office:	Continental House, Kings Hill, Bude, Cornwall, EX23 0LU
3	Account manager name:	Daniel Haggarty
4	Account manager contact number:	01288 271220
5	Account manager email address:	infosec@parentpay.com
Data Protection Officer (DPO) (Art. 37)		
6	Does your company have an allocated Data Protection Officer (DPO)?	Yes
7	DPO name:	*Elliott Lewis*
8	DPO email address:	dpo@parentpay.com
9	DPO contact number:	02476 994 820
Market Place Principle (Art. 3)		
10	Is the EU GDPR applicable to your organisation?	Yes
Principles relating to personal data (Art.5)		
	Do all of your processing activities concerning personal data comply with the following principles? ***All personal data are:***	
11	Processed lawful, fair and in transparent manner?	Yes
12	Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes?	Yes
13	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed?	Yes
14	Accurate and where necessary, kept up to date?	Yes
15	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures?	Yes
Accountability (Art.5 (2))		
16	Are you able to demonstrate compliance (have processes, policies and records) with the principles set out in the previous section?	Yes
Rectification (Art. 16)		
17	Do you have a documented process for correcting inaccurate personal data when asked by the controller?	Yes (via Email request)
Erasure of personal data, right to be forgotten / erased (Art. 17)		
18	Do you have a concept / process for deleting personal data when asked by the controller?	Yes (via Email request)
Restriction of processing (Art. 18)		
19	Do you have a concept / process for restriction of processing personal data upon the controller's request?	Yes (via Email request)
Data portability (Art. 20)		
20	Can you provide data portability for the controller's personal data? That is, can you, at the request of the controller. Provide personal data in a structured, commonly used and machine readable format, and are you able to transmit the data to another controller in case the processing is based on consent or on a contract where the processing is carried out by automated means?	Yes
Data Processing Agreements (DPA) (Art. 28)		
21	Do you have a process in place to inform the controller of any possible use of sub-processors that have access to controller personal data?	Yes, controllers are informed of any sub-processors used by Schoolcomms
22	Can you ensure that only sub-processors of controller personal data are used by providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will ensure protection of the controllers personal data?	Yes
Processing under the authority of the controller or processor (Art. 29)		
23	Are all employees (internal & external) who work with controller personal data, committed to data protection and privacy?	Yes
24	Do you conduct privacy awareness/ training for employees working with controller personal data?	Yes
Records of processing activities (Art. 30)		
25	Is there an overview available concerning all business process/ IT systems processing controller personal data?	Yes
Security of processing of personal data (Art. 24 & 32)		
	Are the following technical and organisation measures in place with relation to controller personal data:	
26	Pseudonymization and encryption following the criticality of personal data?	Yes
27	Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?	Yes
28	Restoration and enabling access to personal data in a timely manner in the event of a physical or technical incident?	Yes
29	Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing?	Yes
Data breach process (Art. 33)		
	When experiencing a data breach containing personal data, is there a process defined to:	
30	Notify the controller as soon as you become aware of the breach?	Yes
31	Document any facts relating to the data breach, its effects and the remedial action taken?	Yes
32	Preserve digital evidence for forensic evidence?	Yes
Other certifications and standards		

33	ISO 27001 Information security	Implementing
34	ISO 9001 Quality management	Uncertified
35	ISO 22301 Business continuity	Uncertified
36	ISO 20001 Service Management	Uncertified
37	PCI DSS	Certified
Data Storage and Management		
38	What controller data do you processes, store or transmit? (if any) *e.g. documents, staff details, customer names, addresses, account numbers, PAN data, audit reports, contact details, system backups, contracts, service management records, source code, multimedia .etc*	Students: Achievement records, behaviour records, assessment records, full name, absence records, club attendance records, assessment reports, pupil premium status, linked contacts, groups from MIS system, dinner payments, club bookings, mobile number, email address, postal address, PIN, class, year group, pre-admission status, Schoolgateway transaction history, MIS ID, phone type (iOS/ Android), roll number, UPN, nationality, gender, FSM status, paypoint card number. Schools: School ID, unique user ID, website URL, description, address, contact number, email address, billing address, billing email address, billing telephone number, purchased Schoolcomms products, DFE number, images, email attachments, bank account details, disbursement history, inbound SMS number, inbound email address, links shared with external websites, MIS system. Staff: Full name, username, memorable data, password, professional email address, role, dinner payments, personal email address, mobile number, PIN, phone type (iOS/ Android), Schoolgateway transaction history. Parents: Full name, email address, mobile number, PIN, linked students, parental responsibility, prime parent status, SIMS priority number, postal address, phone type (iOS/ Android), bank details, Schoolgateway transaction history, messages sent to school via Schoolgateway app. Cashless Retailers: Retailer ID, retailer name, username, memorable data, password.
39	How is data transmitted to and from the controller?	Internet via HTTPS
40	At what frequency is data transmitted to and from the controller?	Whenever an import is run by the data controller themselves.
41	What volume of data is transmitted to and from the controller?	All data required from SIMS is imported during a Schoolcomms import.
42	At what location(s) is controller data stored, transmitted and processed?	Schoolcomms data is stored in Edinburgh and London.
43	Approximately how many people have access (or could have access) to controller data?	50
Policies, processes and procedures		
44	Are organisation policies and procedures with regards to data handling and protection subject to a regular review? (at least annually)	yes
45	Does the organisation have documented agreement and commitment to information security from top management?	yes
HR Controls		
46	Please list all information security polices, processes and procedures established and communicated within your organisation: (please attach supporting evidence) E.g. *Information security policy, Acceptable use policy, Information classification and handling policy, Access control policy, Password policy, Risk management strategy, change control process, Joiners/ leavers/ movers process .etc*	Information security policy, Acceptable use policy, Access control and onboarding/ offboarding policy, BYOD policy, Clear desk policy, Data retention and disposal policy, Development process standards and practices policy, Firewall and Router configuration strategy, Incident response procedure, Information classification and handling policy, Change control process, Data processing agreements, Password policy, Privacy notice, Privacy policy, Patch and vulnerability management strategy, Physical security policy, Social media policy, System build standards policy.
47	Is there a security awareness training program established within the organisation? (If so, please provide details)	Schoolcomms uses Wombat security to conduct security awareness training to all employees. This training is conducted on a regular basis with frequent tests including simulated phishing attacks to ensure that employees are able to identify threats and are able to follow the correct procedures.
48	Are all employees subject to the security awareness training? At what frequency are employees provided with such training?	All employees are subject to security awareness training and this is provided at least on a annual basis
49	Are security awareness training modules kept up to date on latest data protection practices and threat awareness?	Wombat keeps all its modules up to date and adds new modules to cover new topics such as the GDPR. Upon release of these new updates we re-train all employees on that particular subject.
50	Are all employees required to read and agree to security policies in their terms of employment?	All employees are required to read and accept to the security policies during their induction with the company.
51	Is there a mechanism established to ensure employees have read and agreed to security policies applicable to them?	Employees must sign an agreement to confirm they have read and accepted the policies. The policies themselves are also available on our staff portal for easy access at any time.
52	Has the organisation appointed one or more resources to be responsible for information security? If so, please provide roles and responsibilities.	Schoolcomms is part of the ParentPay group which has a dedicated information security team. The team ensures that all business units in the ParentPay group comply with legislation such as GDPR and answer any queries from staff or customers. A member of staff from the security team is available 24/7 in order to respond to any security incidents that may occur.
53	Are new employees subject to background checks prior to employment? If so, please detail what checks are undertaken. E.g. CRB\DBS	Due to the sensitive nature of the data we collect and process, all employees must undergo a Disclosure Barring Service (DBS) check.
Risk Management		
54	Does the organisation maintain an information security asset register?	Yes
54.1	*If so, is the asset register checked on a regular basis for accuracy?*	Yes the register is checked on a quarterly basis to ensure it is up to date.
55	Is there a risk assessment strategy established and in practice?	yes
56	Is risk assessment conducted at a frequency no less than once per year?	yes
57	Are individual information security risks recorded using a risk register?	yes
Incident Management		

58	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
59	Have you experienced any incidents of data loss? If so, please provide reports and supporting information.	No
60	Do you have an established and documented methodology for identifying security incidents?	Yes
Physical Security		
61	Does your organisation conduct regular reviews of the physical security environment and associated physical security risks?	Yes
62	Are business premises suitably robust in structure and protected from unauthorised access with adequate security barriers? (Please provide examples)	Our Worthing office can only be accessed via a secure access control door. All staff are required to wear staff ID badges at all times when on either of our premises.
63	Are any sensitive areas subject to additional security controls? (Please provide details on such controls)	Our datacentres can only be accessed on a by appointment basis and full ID must be presented to onsite security before being allowed access to the server room.
64	What controls are in place to manage, record and secure visitors attending site?	Visitors are requires to sign a visitors book and wear a visitors badge at all times while on the premises.
65	Is a robust process established and practiced for the issue and removal of access permissions for joiners, leavers and those changing roles?	Yes
Network Security		
66	Do you have accurate and maintained network diagrams and documentation detailing endpoints, egress points and traffic flows?	Schoolcomms uses high level architecture diagrams but do not have any network diagrams.
67	Are network changes managed by a defined change control process?	Yes
68	Are Firewall rule bases and/or access control lists reviewed at least every six months for inappropriate/redundant rules?	Yes
69	Is your IP network physically and logically segregated from any other public or private network?	Yes
70	Is the network monitored for suspect anomalies such as bandwidth usage, request counts, endpoint counts, timing of activity, geolocation analysis.	Yes
71	If used, please describe how wireless access is used within the organisation and what wireless network security controls are in place	Wi-fi is available but discouraged in our offices, both offices are routinely checked for rogue access points and the Wi-Fi hotspots are password protected to ensure that no unauthorised access is granted.
72	Do you have a formal process to check for unauthorised\rogue wireless access points?	Yes, routine checks are conducted in both offices to check for rogue access points.
73	Are penetration testing exercises conducted at least every 6-12 months? If so, please provide details (provider, tools, scope).	Annual penetration tests are conducted on the Schoolcomms and Schoolgateway applications. Originally conducted by Pen Test Partners LLP we have since changed provider to NCC. Tests include the web applications, mobile applications and API and include a full TCP and UDP port scan.
Data Encryption		
74	If controller data traverses public or unprotected networks, is it protected by a strong encryption algorithm? If so, what encryption is used?	HTTPS is used for transmitting all data between client machines and our servers, TLS 1.1 and above is implemented to ensure that the data is encrypted during transit.
75	Is controller data encrypted at rest?	No
76	Is there a policy in place to forbid the use of removeable USB Drives, or to enforce encryption of the data when used?	Removable USB devices are forbidden and will not work on company computers.
77	If used, are employee laptops encrypted? (i.e. Bitlocker)	Yes, laptops are encrypted using Bitlocker.
Intrusion Detection and Vulnerability Scanning		
78	Do you have Network and Host Intrusion Detection controls deployed within the infrastructure? If so, please provide details.	Schoolcomms uses the SNORT intrusion detection system to detect suspicious activity on the network. It can also be used to identify and log failed login attempts, brute force attacks and other security events.
79	Do you have vulnerability scanning solutions deployed within the infrastructure? If so, please provide details.	Schoolcomms has implemented the Tenable.io system to scan for vulnerabilities within the infrastructure.
80	Are centrally managed Anti-Virus and Anti-Malware controls deployed within the infrastructure? If so, please provide details.	Schoolcomms uses antivirus solutions provided by Trend Micro on all office workstations and severs.
81	Is there an established and practiced patching strategy in place? If so, please provide details.	A automated patch management strategy is in place using ManageEngine Desktop Central to routinely distribute security patches and updates for Operating Systems and third Party Applications.
82	What measures are in place to detect unauthorised changes within the infrastructure?	ManageEngine Desktop Central is able to monitor and detect any unauthorised changes made to software installations. Snort IDS is able to inform of suspicious changes to the network. Tenable.io will reveal exposed vulnerbilities that are realised due to unauthorised changes.
83	Are procedures documented and practiced to ensure the regular review of log and security management platforms?	Yes
Access Control		
84	Are access controls methods in place to record and authorise permissions and access levels to all systems and data throughout the enterprise?	Yes an action control register is kept and maintained. Access controls prevent unauthorised access to systems.
85	Are access levels reviewed on a regular basis? If so, at what frequency?	Access controls are reviewed at least bi-annually to ensure they are kept up to date.
86	Are access levels granted according to principle of least privilege?	Yes
87	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 + compensating controls	All accounts used within Schoolcomms attribute to a uniquely identifiable staff member. The only accounts that are shared are School "Support User" accounts used by members of the support team and are individual to each school. The usage of these accounts is restricted to only Support team personnel and audit logs are recorded to prevent misuse.
88	Are failed and successful logons monitored and logged throughout the environment? Please detail any exceptions + compensating controls	Failed logins to internal systems are recorded and users will be locked out after a varying number of attempts. Access to the Schoolcomms and Schoolgateway products is also denied after several failed login attempts.

89	Are password criteria for networks, operating systems and applications sufficiently complex? (see below, please detail exceptions + compensating controls) *Passwords must be at least 8 characters in length *Passwords must be a combination of alpha and numeric characters *Passwords must expire every 30 days *Controls should prevent reuse of passwords for at least 5 generations *Users must change passwords upon access to the system for the first time	Schoolcomms has a Password policy which ensures that all staff members are aware of the importance of a strong password. Our policy ensures a strict password criteria is met including being over 10 characters in length and containing at least one upper case letter and one special character. Passwords must be changed every 3 months and old passwords cannot be re-used. Users are also prompted to change their password upon first login.
90	What security measures are in place to prevent brute-force type password guessing attacks? E.g. account lockouts and\or captcha forms.	Account lockouts are in place to prevent brute force attacks. Accounts will be locked after a number of failed login attempts (between 3 and 5 depending on the system). .
91	Are all access credentials adequality protected in transit and storage? i.e. not transmitted or stored in clear text under any circumstances?	The password policy forbids the storage of passwords via plaintext documents. Employees are encouraged to use one of two authorised password manager applications to safely and securely store and share passwords internally.
92	Are passwords audited on a regular basis to ensure compliance with policy and best practice?	Yes
93	Are all passwords adequately hashed? (with salt?) or encrypted? Please detail what algorithms are in use across the infrastructure.	Passwords are currently hashed with SHA1, at present this is without salt, however a future project on our roadmap will be to improve credential encryption and apply salt when encrypting credentials.
94	Are inactive\stale accounts automatically purged or disabled? If so, what is the threshold for accounts to be removed or disabled?	Staff accounts are deleted upon the termination of employment. School accounts are archived for a maximum of 5 months before the account is permanently disabled.
95	How are logon sessions managed securely?; for example concurrent sessions, inactive sessions, long duration sessions.	All logon sessions are set to time-out after a set period of time. This amount of time varies between systems and users are required to log back in after time-out.
96	Is there a policy in place to ensure workstations are locked while unattended and an automatic lockout out after a period of inactivity?	The clear desk policy requires that all staff members lock their workstations when not at their desks.
97	Is the use of vendor supplied default passwords and weak passwords adequately prevented? How is this achieved?	Supplier and vendor default passwords are changed by tech-ops before access is granted to staff members.
98	Are all physically remote access channels into the infrastructure (such as VPN) protected by multi-factor authentication systems?	Access to secure systems and our VPN requires two factor authentication.
99	Is appropriate logging and monitoring in place to ensure remote access user activity is captured and reviewed?	yes
100	Are administrative permissions removed from employees workstations unless specifically required and authorised?	yes
Data Protection		
101	**Is there a documented process to be followed in the following scenarios?**	
101	Controller data is lost, damaged, destroyed or otherwise unusable.	yes
101	Controller data has been (or may have been) subject to unlawful processing	yes
101	Controller data is deemed to be at increased risk due to changes or incidents.	yes
102	Are you registered with the UK Information Commissioner (or equivalent) If so, please provide details (registration number)	yes ICO registration: Z8261740
103	What controls are in place to manage office working locations such as clear desk policy, secure disposal, privacy screens. How is this policed?	A clear desk policy is enforced as well as a data retention and disposal policy, routine checks are performed by the security team to ensure compliance.
104	What controls are in place to manage out-of-band access to sensitive information? Such as database access by administrators.	Database access is strictly controlled and monitored. Acess is protected by multi-factor-authentication, available only via whitelisted dedicated management nodes, and subject to full audit trail logging. Only Database administrators and senior members of the IT tech team have any database access.
105	What controls are established to manage the use of mobile devices?	The use of company provided mobile phones is limited to email access only, and management controls are applied - including encryption, PIN access and MDM capabilities. Company laptops are subject to full disk encryption and remote management controls.
Business Continuity		
106	Do you have a company policy and strategy for business continuity?	Yes, ParentPay group has a documented business continuity strategy.
107	Are business continuity and disaster recovery plans tested on a regular basis? If so, please provide details and supporting evidence.	Schoolcomms operations and infrastructure is fully resillient and prepared to handle a comprehensive set of serious failures. These are excercised regularly through various mechanisms.
108	Do critical systems and infrastructure have a disaster recovery solution available within a separate physically remote location.	Schoolcomms operates a secondary datacentre for use in a Disaster scenario. All critical systems are frequently backed up and replicated to the secondary site.
109	Are backup and restore procedures tested on a regular basis? At what frequency, and to what extent does this occur?	Yes, backup and restore procedures are conducted on an regular basis. Full database backups are typically tested on at least a monthly basis.
110	What is the recovery point objective and recovery time objective for disaster recovery? (if available)	Recovery point objective is 5 minutes. Recovery time objective will vary depending on the nature of the disaster. A full data recovery can be completed within 12 hours.
111	Are capacity management processes in place and practiced? If so, please provide detail on how capacity is managed.	System performance and resoruces are closely monitored on a 24x7x365 basis. Activity and utilisation is reviewed over time and the system is scaled accordingly to manage forecasted requirements.
Software Development		
112	Are development processes and practices defined and documented, including security consideration and best practices?	Yes
113	Does the organisation adopt the 'privacy by design' approach to application data protection.	Yes
114	Are development team members made aware of the organisations development processes and requirements? How is this communicated?	Yes, via the development process, standards and procedures policy.
115	Are software developers trained in secure coding methods and practices? If so, please provide details.	Yes, developers are provided annual training in secure development methods and practices.
116	Is code review conducted for all new developments and software changes independent from that of the original developer?	yes
117	Are internally developed applications (including web applications) subject to manual penetration testing every 6-12 months?	yes

118	Are security controls implemented throughout software development and continuous integration systems? If so, please provide details.	Developers are advised to be familiar with the OWASP top 10 web application risks and work to ensure these risks are mitigated or prevented. The development team work to a "privacy by design" approach which ensures that data is secure and meets current EU GDPR requirements for data transparency, minimisation and retention.
119	Are development and testing environments adequate separated from live\production environments? Please provide details.	Yes, development and test environments are kept separated from the live production environments. No test data or live data is shared between these two environments.
120	Where applicable, how is data protected within testing and development environments? E.g. load testing and acceptance testing data stores.	No live data is used at any stage of the development or testing stages. Instead test data is provided in the form of a fictional demonstration school provided by Capita.
121	Are internally developed products subject to standard security requirements surrounding authentication, validation and auditing? Please detail what these specific requirements are.	Yes, all products must be developed with a number of security requirements in consideration, including but not limited to: - Does the application enforce adequate password complexity? - Are users prompted to reset their password on a regular basis? - Does the application support modular / role based security? - Successful and failed logins should be recorded - Common passwords should be prevented (such as those based on usernames) - Are all user input fields subject to strict validations checks for size\ range, format and content? - Security must be enforced from a server side, not a client side.
Third Parties		
122	Is controller data shared with any third parties or subcontractors? (If so, please provide details).	School data may be shared with third parties in order to carry out sub-processing activities such as balance updates and payment processing. School and parent data is also shared with AQL & Esendex for the purpose of distributing SMS messages and SendGrid for the purpose of sending emails.
123	Are any third parties or sub-processors located outside of the UK or European Economic Area (EEA)? (Please provide details).	No
124	Is there a process implemented to ensure all third parties and sub-processors are GDPR compliant before providing controller data?	Yes, third-parties and sub-processors are required to fill out a security RFI such as this one in order to verify their GDPR compliance.
125	How is the security of data maintained when sharing with a third party or sub-processor?	Data is always transmitted over encrypted channels and subject to Data Processing Agreements; mandating the use of appropriate technical and organisational measures to protect data.
126	Are non-disclosure agreements in place with all third parties that may have access to sensitive information and\or intellectual property?	Yes
127	Do you conduct risk assessments of external 3rd parties prior to allowing them access to your systems? (If so, please provide details)	Yes, any third parties that require access to Schoolcomms systems undergo a Risk Assessment and any new projects are subject to a Data Protection Impact Assessment (DPIA) to ensure that any risks that could arise from granting access to data have been identified and mitigated.
128	Are security controls required in your contracts with external 3rd parties? If so, please provide details.	ParentPay group provides a supplier and third party management policy which contains a number of security requirements that 3rd parties must meet before processing is allowed to commence. This includes agreeing to a number of policies such as Acceptable use, Information & Data handling, Anti-bribery & corruption, and security incident handling.
129	Do you maintain the right to verify implementation of 3rd party controls at least annually?	Yes
Signature		
130	Date of Completion:	17-05-2018