MarvellousMe Compliance with General Data Protection Regulation

MarvellousMe takes the protection and security of personal data extremely seriously.

We follow industry recommended best practices with regards to data security and the privacy of personal data, with our technology partner operating our service to ISO 9001:2015, ISO 27001:2017 and being Cyber Essentials certified.

With the General Data Protection Regulation (GDPR) coming into effect in May 2018, we have taken technical and organisations measures to ensure that we comply with GDPR, and updated our policies and procedures.

What we have done to comply with GDPR

As an organisation that handles personal data including sensitive personal data, MarvellousMe is committed to ensuring that we are compliant with GDPR. Some of the steps we have taken include:

- ✓ Mapping and documenting data handled by us, including:
    - identifying the personal and sensitive data held;
    - where the data is stored, how the data is used and with whom the data is shared;
    - establishing where the data came from and identifying the legal basis for holding and processing it; and
    - reviewing our standard retention periods.
- ✓ Analysing GDPR requirements against our current processes and policies and made changes to our products, processes and documentation in line with requirements including:
    - reviewing and updating our Terms & Conditions, Privacy Policy and Terms of Use to comply with the requirements of GDPR;
    - reviewing and updating the contract with our sub-processor, setting out each party's respective responsibilities under GDPR; and
    - reviewing how we communicate with schools.
- ✓ Undertaking a review of our security measures to ensure systems are robust to identify any potential risks of non-compliance or any weaknesses in our data storage and handling systems;
- ✓ Providing training to all staff on the requirements of GDPR and MarvellousMe data privacy procedures;
- ✓ Ensuring that procedures are in place to deal with individual's enhanced rights under GDPR, including ensuring we can respond to all types of data subject requests within a timely manner.

Our platform and service highlights

The MarvellousMe platform is continually being updated to provide new features to customers and combat an ever-evolving landscape of internet threats. It is built using modern architectural principles and is frequently assessed to ensure that your data remains safe.

We have provided the summary below to answer common questions, and in line with the Cloud Software Services for Schools Supplier Self-Certification Checklist provided by the Department of Education and Schools Commercial team.

- ✓ Our platform is operated across multiple, Tier 4 data centres which means that all components are fully fault-tolerant, including (but not limited to) internet uplinks, storage, cooling, power and servers.
- ✓ Our data centre partner holds over 15 compliance certifications and has been approved for use on over 20 governmental frameworks. Our primary data-centre also features direct connectivity with JANET, the UK's Research and Education Network, for the best possible experience from connected education establishments. Access to this environment is tightly controlled and limited to a small number of Sec-DevOps engineers and senior developers based in the UK.
- ✓ We act as the Data Processor, acting only according to the instructions of the Data Controller (the school).

- ✓ We prohibit personal data or metadata being shared across other services, and only share data with our sub-processor (our technology partner). We do not share data with any other third parties.
- ✓ Access to the service is via a unique login ID and password. All aspects of the service, including authentication, are delivered via HTTPS.
- ✓ Sensitive data such as passwords are encrypted. Other data is not encrypted but is held in a secure data centre.
- ✓ All transit of data is via secure, encrypted methods and at no time is data transferred between data centres without encryption. Our email traffic uses SMTPS to secure traffic using TLS.
- ✓ We strictly limit the amount of personal data stored and ensure that it is only retained for the minimum duration necessary.
- ✓ Users can request a copy of their own data. This will be provided to them within 30 days of their request.
- ✓ We destroy all the copies of a school's data within 90 days of the end of a contract, or upon request during the contract.
- ✓ Our service is backed up as a minimum every 24 hours. This ensures that all user data can be restored if required.
- ✓ Data is exclusively hosted within the European Economic Area.
- ✓ We do not serve advertisements or carry-out any advertisement-related data mining.
- ✓ We do not use or pass on any personal data or meta data for any commercial purpose.

Our policies and procedures

We have updated our policies and procedures to comply with GDPR:

- ✓ We have updated our School Terms and Conditions, incorporating the government's own GDPR Contract Clauses (published by the Crown Commercial Service – Dec 2017) in our Data Processing Schedule with school clients.
- ✓ We have updated our Sub-Processor agreement, ensuring that any third-party processing personal data on our behalf is GDPR compliant.
- ✓ We have updated our Privacy Policy and Terms of Use to comply with GDPR. These can be found on our website.

Should you have any questions about our service, our platform security, data privacy or conformity to GDPR, please contact adrian@marvellousme.com

Kind regards

Adrian Burt
Founder and Director
April 2018

MarvellousMe School Terms and Conditions

Data Processing Schedule

BACKGROUND

(A) MarvellousMe takes the protection and security of the personal data of users, pupils and clients extremely seriously.
(B) This Schedule sets out the obligations of the parties whether as data collectors or data processors and to ensure that both parties operate within the Data Protection Act and General Data Protection Regulation (GDPR).
(C) The terms of this Schedule are agreed by the parties.

1. Definitions

"Agreement"	these terms which are intended to be and shall be incorporated into the MarvellousMe School Terms and Conditions and Subscription Form (collectively the Terms) as agreed and entered into by the parties;
"Data Protection Legislation"	any legislation relating to the processing, privacy and use of personal data, as applicable to MarvellousMe, you and/or the Services being provided under the Agreement, including: the Data Protection Act 1998 (DPA 98) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all other applicable legislation implementing European Community Directives 95/46 and 2002/58, and any subsequent European Union legislation, including the EU General Data Protection Regulation 2016/679, once applicable ('the GDPR') and any applicable national legislation implementing or supplementing the GDPR, in relation to the protection of personal data and/or any corresponding or equivalent national legislation in any relevant jurisdiction (once in force and applicable).
"Data Protection Impact Assessment"	an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Subject, **Personal Data**, **Personal Data Breach**, **Processor"**	each takes the meaning given in the Data Protection Legislation;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach;
"Data Subject Access Request"	a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
"Law"	means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Contractor is bound to comply;
"LED"	Law Enforcement Directive *(Directive (EU) 2016/680)*
"MarvellousMe Personnel"	means all directors, officers, employees, agents, consultants and contractors of MarvellousMe and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement;
"Party"	a Party to this Agreement;
"Protective Measures"	appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity,

availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it; and

"Sub-processor" any third Party appointed to process Personal Data on behalf of MarvellousMe related to this Agreement.

2. Data Protection

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation:

a) MarvellousMe is the Data Processor;

b) the only processing that MarvellousMe is authorised to do is to process the personal data of pupils, parents and teachers in accordance with the Terms and this Agreement, and

You warrant to MarvellousMe that you are the Data Collector and that you have a lawful right and permission to collect and to pass any Personal Data that is the subject of this Agreement to MarvellousMe to be processed.

1.2 MarvellousMe shall notify you immediately if it considers that any of your instructions infringe the Data Protection Legislation.

1.3 MarvellousMe shall provide all reasonable assistance to you in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may include:

a) a systematic description of the envisaged processing operations and the purpose of the processing;

b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

c) an assessment of the risks to the rights and freedoms of Data Subjects; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4 MarvellousMe shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

a) process that Personal Data only in accordance with Schedule A, unless MarvellousMe is required to do otherwise by Law. If it is so required, MarvellousMe shall promptly notify you before processing the Personal Data unless prohibited by Law;

b) ensure that it has in place Protective Measures that are appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures.

c) ensure that:

(i) MarvellousMe Personnel does not process Personal Data except in accordance with this Agreement (and in particular Schedule A);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any MarvellousMe Personnel who have access to the Personal Data and ensure that they:

1.4.c.ii.1 are aware of and comply with MarvellousMe's duties under this clause;

1.4.c.ii.2 are subject to appropriate confidentiality undertakings with MarvellousMe or any Sub-processor;

1.4.c.ii.3 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by you or as otherwise permitted by this Agreement; and

1.4.c.ii.4 have undergone adequate training in the use, care, protection and handling of Personal Data;

d) not transfer Personal Data outside of the **EEA** unless your prior written consent has been obtained and the following conditions are fulfilled:

(i) you or MarvellousMe has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by you;
(ii) the Data Subject has enforceable rights and effective legal remedies;
(iii) MarvellousMe complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses reasonable endeavours to assist you in meeting its obligations); and
(iv) MarvellousMe complies with any reasonable instructions notified to it in advance by you with respect to the processing of the Personal Data;

e) at your written direction, delete or return Personal Data (and any copies of it) to you on termination of the Agreement unless MarvellousMe is required by Law to retain the Personal Data.

1.5 Subject to clause 1.6, MarvellousMe shall notify the Customer immediately if it:

a) receives a Data Subject Access Request (or purported Data Subject Access Request);
b) receives a request to rectify, block or erase any Personal Data;
c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
d) receives any communication from the Information Commissioner or any other competent regulatory authority in connection with Personal Data processed under this Agreement;
e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or becomes aware of a Data Loss Event.

1.6 MarvellousMe's obligation to notify under clause 1.5 shall include the provision of further information to you in phases, as details become available.

1.7 Taking into account the nature of the processing, MarvellousMe shall provide full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 1.5 (and insofar as possible within the timescales reasonably required by you) including by promptly providing:

a) you with full details and copies of the complaint, communication or request;
b) such assistance as is reasonably requested by you to enable you to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
c) you, at your request, with any Personal Data it holds in relation to a Data Subject;
d) assistance as requested by you following any Data Loss Event;
e) assistance as requested by you with respect to any request from the Information Commissioner's Office, or any consultation by you with the Information Commissioner's Office.

1.8 MarvellousMe shall maintain complete and accurate records and information to demonstrate its compliance with this clause.

1.9 MarvellousMe shall allow for audits of its Data Processing activity by you or your designated auditor.

1.10 MarvellousMe shall designate a data protection officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, MarvellousMe shall:

a) notify you in writing of the intended Sub-processor and processing;
b) obtain your written consent;
c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Schedule such that they apply to the Sub-processor; and
d) provide you with such information regarding the Sub-processor as you may reasonably require.

1.12 MarvellousMe shall remain liable for all acts or omissions of any Sub-processor and shall use reasonable efforts to obtain an indemnity from the Sub-Processor for all acts or omissions.

1.13 You may, at any time on not less than 30 Working Days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. You may, on not less than 30 Working Days' written notice to MarvellousMe, amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Schedule A – Processing, Personal Data and Data Subjects

1. MarvellousMe shall comply with any further written instructions with respect to processing by you.

2. Any such further instructions shall be incorporated into this Schedule.

Description	**Details**
Data Controller	*The party to the Terms to which this Schedule applies.*
Data Processer	MarvellousMe Ltd, a company incorporated under the laws of England with registered number 08782237, whose registered address is Mousetows, Mouse Lane, Steyning, West Sussex BN44 3LP, UK (**MarvellousMe**). *Sub-processer is* CloudThing Limited, a company incorporated under the laws of England with registered number 07510381, whose registered address is 14 The Square, Feckenham, Redditch, Worcestershire, B96 6HR, UK.
Subject matter of the processing	*The subject matter and duration of the processing of the Protected Data are set out in the Terms entered into by the parties.*
Duration of the processing	*For the duration of the Terms, subject to termination and/or periodic review.*
Nature and purposes of the processing	*MarvellousMe collects and stores personal data from registered clients and users of the MarvellousMe website and apps to enable schools to inform parents and guardians on their children's progress and achievements, and to monitor communications sent home from school staff.*
Type of Personal Data	*To provide the core service, the following data will be processed:* - *Pupil first and last name* - *Pupil UPN (Unique Pupil number)* - *Pupil School Registration Group* - *Pupil School Year* - *Teacher/School Staff name* - *Teacher/School Staff email* - *Teacher/School Staff class(es) /group(s)* - *Parent/Guardian name* - *Parent/Guardian email* - *Parent/Guardian phone/device ID* *Optionally, additional pupil data, if provided by the client, may be processed to support additional school reporting requirements, such as:* - *Special Educational Needs* - *Applicability for Pupil Premium / or Free School Meals / Service Allowance etc.* - *House or Team membership* - *Ethnicity* - *Gender*
Categories of Data Subject	*The categories of data subjects: teachers and school employees, parents, guardians and pupils.*

Plan for return and destruction of the Protected Data once the processing is complete UNLESS requirement under law to preserve that type of data	*The data will be processed for the duration of the Terms agreed and then returned to the Data Controller and/or destroyed as required or set out in this Agreement, or anonymised or* pseudonymised*.*