DATA PROCESSING AGREEMENT

(SKL as Processor and Customer as Controller)

THIS DATA PROCESSING AGREEMENT forms part of the Supply of Service Agreement (the "**Service Agreement**") between Mesa Public Schools and SportsKey Ltd. (SKL) (together as the "**Parties**").

WHEREAS

This Data Processing Agreement ("**Agreement**") sets out the additional terms, requirements and conditions on which SKL will process Personal Data when providing services under the Service Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors.

IT IS HEREBY AGREED

1. DEFINITIONS AND INTERPRETATION

Save for following definitions and rules of interpretation which apply in this Agreement, all other definitions are as provided for under the Service Agreement.

1.1 Definitions:

"**Applicable Law**"	means (i) any and all laws, statutes, regulations, by-laws, orders, ordinances and court decrees that apply to the performance and supply of the services under the Service Agreement or the Processing of the Personal Data, and (ii) the terms and conditions of any applicable approvals, consents, exemptions, filings, licences, authorities, permits, registrations or waivers issued or granted by, or any binding requirement, instruction, direction or order of, any applicable government department, authority or Customer having jurisdiction in respect of that matter.
"Authorised Persons"	means the persons or categories of persons that the Customer authorises to give SKL personal data processing instructions as identified in Appendix A
"Business Purposes"	means the services described in the Service Agreement or any other purpose specifically identified in Appendix A.
"Data Subject"	means an individual who is the subject of Personal Data.
"Personal Data"	means any information relating to an identified or identifiable natural person that is processed by SKL as a result of, or in connection with, the provision of the services under the Service Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For the purposes of the agreement between Mesa Public Schools and Sports Key, personally identifiable data is not collected for any students or staff of MPS. The data collected is for "end-users" of the school's sports facilities – eg, name, business address, and phone number.

"Processing, processes and process"	means either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.
"Data Protection Legislation"	means all applicable privacy and data protection laws including the General Data Protection Regulation (*(EU) 2016/679*) and any applicable national implementing laws, regulations and secondary legislation in Ireland relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time.
"**DP Losses"**	means all liabilities, including all: (a) costs (including legal costs), claims, demands, actions, settlements, ex-gratia payments, charges, procedures, expenses, losses and damages (including relating to material and non-material damage); and (b) to the extent permitted by Applicable Law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a court or regulatory authority; (ii) compensation to a Data Subject ordered by a court or regulatory authority; and (iii) the costs of compliance with investigations by a regulatory authority.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"Processing Instructions"	means the Customer's instructions provided by the Customer to SKL from time to time or as set out in the Agreement.
"Standard Contractual Clauses (SCC)"	means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.

1.2 This Agreement is subject to the terms of the Service Agreement and is incorporated into the Service Agreement. Interpretations and defined terms set forth in the Service Agreement apply to the interpretation of this Agreement.

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 A reference to writing or written includes faxes but not email.

1.5 In the case of conflict or ambiguity between:

1.5.1 any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

1.5.2 the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

1.5.3 any of the provisions of this Agreement and the provisions of the Service Agreement, the provisions of this Agreement will prevail.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 The Customer and SKL acknowledge that for the purpose of the Data Protection Legislation, the Customer is the controller and SKL is the processor.

2.2 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to SKL.

2.3 Appendix A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which SKL may process to fulfil the Business Purposes of the Service Agreement.

3. SKL OBLIGATIONS

3.1 SKL will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions from Authorised Persons. SKL will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. SKL will notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.

3.2 SKL will comply with any Customer request or instruction from Authorised Persons requiring SKL to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 SKL will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires SKL to process or disclose Personal Data, SKL must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 SKL will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of SKL processing and the information available to SKL, including in relation to Data Subject

rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

4. SKL EMPLOYEES

4.1 SKL will ensure that all employees:

4.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

4.1.2 are aware both of SKL duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

5. SECURITY

5.1 SKL must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Appendix B.

5.2 SKL must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. PERSONAL DATA BREACH

6.1 SKL will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable.

6.2 SKL will within 24 hours and without undue delay notify the Customer if it becomes aware of:

6.2.1 any accidental, unauthorised or unlawful processing of the Personal Data; or

6.2.2 any Personal Data Breach.

6.3 Where SKL becomes aware of 6.2.1 and/or 6.2.2 above, it shall, without undue delay, also provide the Customer with the following information:

6.3.1 description of the nature of 6.2.1 and/or 6.2.2, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

6.3.2 the likely consequences; and

6.3.3 description of the measures taken, or proposed to be taken to address (a) and/or (b), including measures to mitigate its possible adverse effects.

6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. SKL will reasonably co-operate with the Customer in the Customer's handling of the matter, including:

6.4.1 assisting with any investigation;

6.4.2 providing the Customer with physical access to any facilities and operations affected;

6.4.3 facilitating interviews with SKL employees, former employees and others involved in the matter;

6.4.4 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

6.4.5 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

6.5 SKL will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 SKL (or any subcontractor) must not transfer or otherwise process Personal Data outside the European Economic Area ("**EEA**") without obtaining the Customer's prior written consent.

7.2 Where such consent is granted, SKL may only process, or permit the processing, of Personal Data outside the EEA under the following conditions:

7.2.1 SKL is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. SKL must identify in Appendix A the territory that is subject to such an adequacy finding; or

7.2.2 SKL participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that SKL (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation (*(EU) 2016/679*). SKL must identify in Appendix A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and SKL must immediately inform the Customer of any change to that status; or

7.2.3 the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Appendix A.

7.3 If the Customer consents to appointment by SKL located within the EEA of a subcontractor located outside the EEA in compliance with the provisions of clause 8, then

the Customer authorises SKL to enter into SCC with the subcontractor in the Customer's name and on its behalf. SKL will make the executed SCC available to the Customer on request.

8. SUBCONTRACTORS

8.1 SKL may only authorise a third party (subcontractor) to process the Personal Data if:

8.1.1 the Customer is provided with an opportunity to object to the appointment of each subcontractor within 14 days after SKL supplies the Customer with full details regarding such subcontractor;

8.1.2 SKL enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of such contracts;

8.1.3 SKL maintains control over all Personal Data it entrusts to the subcontractor; and

8.1.4 the subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.2 Those subcontractors approved as at the commencement of this Agreement are as set out in Appendix A. SKL must list all approved subcontractors in Annex A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under such written agreement, SKL remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.4 The Parties consider SKL to control any Personal Data controlled by or in the possession of its subcontractors.

8.5 On the Customer's written request, SKL will audit a subcontractor's compliance with its obligations regarding the Customer's Personal Data and provide the Customer with the audit results.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD PARTY RIGHTS

9.1 SKL must, at the cost of the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

9.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

9.1.2 information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

9.2 SKL must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 SKL must notify the Customer within 4 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 SKL will endeavour to give the Customer co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 SKL must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this Agreement or as required by law.

10. TERM AND TERMINATION

10.1 This Agreement will remain in full force and effect so long as:

10.1.1 the Service Agreement remains in effect, or

10.1.2 SKL retains any Personal Data related to the Service Agreement in its possession or control ("**Term**").

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Service Agreement in order to protect Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Service Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within one month, they may terminate the Service Agreement on written notice to the other party.

11. DATA RETURN AND DESTRUCTION

11.1 At the Customer's request, SKL will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Service Agreement for any reason or expiry of its term, SKL will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this Agreement in its possession or control, except for one copy that it may retain and use for six months for audit purposes only and unless retention is required by law.

11.3 If any law, regulation, or government or regulatory body requires SKL to retain any documents or materials that SKL would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 SKL will certify in writing that it has destroyed the Personal Data within 28 days after it completes the destruction.

12. RECORDS

12.1 SKL will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Customer, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 ("**Records**").

13. AUDIT

13.1 SKL will permit the Customer and its third-party representatives to audit SKL compliance with its Agreement obligations, on at least 21 days' notice, during the Term. SKL will give the Customer and its third-party representatives all assistance, as it can reasonably afford to give, to conduct such audits. The assistance may include, but is not limited to:

13.1.1 physical access to, remote electronic access to, and copies of the Records and any other information held at SKL premises or on systems storing Personal Data;

13.1.2 access to and meetings with any of SKL personnel reasonably necessary to provide all explanations and perform the audit effectively; and

13.1.3 inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

13.2 The notice requirements in clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach occurred or is occurring, or SKL is in breach of any of its obligations under this Agreement or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or SKL becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, SKL will:

13.3.1 within 5 days of the triggering event, conduct its own audit to determine the cause;

13.3.2 produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

13.3.3 provide the Customer with a copy of the written audit report; and

13.3.4 remedy any deficiencies identified by the audit within 21 days.

13.4 At the Customer's written request, SKL will:

13.4.1 At least once a year, SKL will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement.

14. WARRANTIES

14.1 SKL warrants that considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or

destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

(b) the nature of the Personal Data protected; and

(c) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The Customer warrants and represents that:

14.2.1 the processing of Personal Data by the Customer will be carried out in accordance with Data Protection Legislation;

14.2.2 SKL is entitled to process the Personal Data pursuant to the Service Agreement for the purpose of providing the services thereunder and such use will comply with Data Protection Legislation;

14.2.3 SKL is entitled to access any Personal Data provided by the Customer or the User to any payment provider platform used for the purpose of paying the Fees. Where applicable, the Customer has obtained the necessary approval of any User in this regard;

14.2.4 all Personal Data provided by the Customer to SKL is necessary, accurate and up-to-date; and

14.2.5 all Processing Instructions shall at all times be in accordance with Data Protection Legislation.

15. INDEMNITY AND LIMITATION OF LIABILITY

15.1 Subject to clause 15.2, the Customer shall indemnify and keep indemnified SKL in respect of all DP Losses suffered or incurred by, awarded against or agreed to be paid by SKL and any Sub-Processor arising from or in connection with any:

15.1.1 non-compliance by the Customer with Data Protection Legislation;

15.1.2 processing carried out by SKL or any Sub-Processor pursuant to any Processing Instruction that infringes Data Protection Legislation; or

15.1.3 breach by the Customer of any of its obligations under this Agreement.

15.2 The Customer shall not be liable for any DP Losses under this Agreement directly resulting from SKL's breach of this Agreement.

15.3 To the maximum extent permitted by applicable law, SKL's total aggregate liability in contract, tort (including negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement or any collateral contract shall in all circumstances be limited to 100% of the fees paid or payable during the 12 months preceding the event triggering SKL's liability.

16. NOTICE

16.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing.

16.2 Clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16.3 A notice given under this Agreement is not valid if sent by email.

Education Technology

Apr 18, 2024

Director of Application & Systems Development

Nathan Myers

namyers@mpsaz.org

APPENDIX A
Personal Data Processing Purposes and Details

Subject matter, nature and purpose of processing: the provision of the services in accordance with the Service Agreement

Duration of Processing: the term under the Service Agreement and any agreed extension by the parties

Personal Data Categories: names, email addresses, residential / business addresses, contact numbers

Authorised Persons: any employee authorised by SKL

Data Subject Types: the Customer's employees and the users of the Customers' facilities

APPENDIX B
Security measures

Sub-Processors

SKL uses third-party sub-processors to operate its products. Each of these sub-processors provides their own GDPR-compliant data processing agreement. The following is a list of sub-processors currently in use:

- Heroku (Cloud computing provider) – https://heroku.com
- Amazon Web Services (Cloud computing provider) – https://aws.amazon.com
- Stripe (Payment processing service) – https://stripe.com
- Intercom (Customer support service) - https://www.intercom.com/
- CloudFlare (Network Infrastructure provider) – https://cloudflare.com
- Rollbar (Error reporting service) - https://rollbar.com/

Data Center Security

SKL hosts its service with a third-party infrastructure provider (Heroku/Salesforce). Their physical and environmental security controls are certified and audited for SOC 1, 2 and 3 as well as ISO 27001, 27017 and 27018. SKL's own employees do not have physical access to any servers. SKL uses its cloud providers' access control mechanisms, such as firewalls, to only allow network traffic using authorized protocols to and from its product.

Protection from Data Loss

All databases run on highlight redundant server infrastructure and are backed up in real time with rollback and restore facilities for any point within the last 7 days.

Application Security

All of SKL's systems (including its product and website) are accessible only via TLS (Transport Layer Security) encrypted requests. Customer data is stored in multi-tenant storage systems which can be accessed only through SKLs' product's user interface and API. Customers who interact with SKL's product via the user interface or API must authenticate with a username and password to access any non-public data. All passwords are stored in secure one-way encrypted form. All other data is stored encrypted at rest. SKL's product implements an authorisation model to ensure that only the appropriately assigned individuals can access relevant features, settings, and data. Authorisation checks are performed after authentication for every request to SKL's system through the user interface and API.

Operational Security

Any software updates to SKL's system undergoes a rigorous, multi-step process of both manual and automated testing and analysis, to ensure security, including code reviews, static code analysis, and checks against known security vulnerabilities of third-party software packages as published by the CVE security vulnerability database. In addition, SKL uses a dedicated security and attack mitigation provider (CloudFlare) to detect and mitigate common attacks such as DDoS. External access to SKL's systems and data is protected by its respective cloud providers' security provisions. As a policy, SKL enforces two-factor authentication (2FA) for all of its employees to gain access to these systems.

Signature:

Email: nmsietsema@mpsaz.org