

Impact Netball Club Data Processing Agreement

Standard version: 1.0

Published: 19 September 2026

This is Pegasus Sports Media Limited's standard Data Processing Agreement for schools and clubs using Impact Netball Club. It becomes binding when signed, electronically accepted or expressly incorporated into the applicable customer agreement. The online copy does not by itself identify or bind a particular customer.

This Data Processing Agreement (the **DPA**) forms part of the agreement for the Impact Netball Club service (the **Main Agreement**) between:

1. the customer school or club identified in the Main Agreement (the **Controller**); and
2. **Pegasus Sports Media Limited**, 5 Swan Place, Westerham, Kent TN16 1UF, United Kingdom (the **Processor**).

The effective date is the date this DPA is last signed or accepted, or the date on which the Main Agreement incorporates it.

1. Scope and Roles

1.1 The Controller determines the purposes and essential means of processing athlete, team, fixture, game-event and performance data entered into or generated through Impact Netball Club.

1.2 The Processor processes that personal data on the Controller's behalf only to provide, secure, support and maintain Impact Netball Club and in accordance with the Controller's documented instructions, including this DPA, the Main Agreement and instructions capable of being retained in written form.

1.3 Pegasus Sports Media acts as an independent controller, rather than a processor, for personal data for which it determines the purposes and means of processing, including user-account administration, subscription and billing administration, customer support, service security, fraud prevention, legal compliance and commercial relationship management. That processing is governed by the Impact Netball Club Privacy Notice and falls outside the processor obligations in this DPA.

1.4 If an authorised user is permitted to access more than one organisation, each organisation's access and data remain separately permissioned. Access to one organisation does not authorise access to another.

2. Controller Instructions and Responsibilities

2.1 The Processor will process personal data only on documented instructions from the Controller, including for international transfers, unless UK law requires otherwise. Where legally permitted, the Processor will notify the Controller before carrying out legally required processing.

2.2 The Controller is responsible for:

- having a lawful basis for the personal data it submits or instructs the Processor to process;
- providing required privacy information to athletes, parents or guardians, staff and other affected individuals;
- ensuring its instructions comply with applicable data-protection law;
- granting access only to authorised users and keeping permissions current;
- not entering medical, safeguarding or other special-category data unless expressly agreed in writing and supported by an appropriate lawful basis and safeguards; and

- protecting exported reports and data copied outside the service.

3. Confidentiality

3.1 The Processor will ensure that each person authorised to process Controller personal data is subject to an appropriate contractual or statutory duty of confidentiality and accesses it only as necessary for their role.

4. Security

4.1 Taking account of the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the risks to individuals, the Processor will maintain appropriate technical and organisational measures. The measures currently applicable are described in Schedule 2.

4.2 The Controller acknowledges that security is a shared responsibility and will maintain suitable device passcodes, operating-system updates, account security, authorised-user controls and physical security for devices used with the service.

5. Sub-processors

5.1 The Controller gives general written authorisation for the Processor to use the sub-processors listed in Schedule 3 for the stated purposes.

5.2 The Processor will maintain an up-to-date sub-processor list and notify the Controller's administrative contact in writing of an intended addition or replacement sufficiently in advance to allow a reasonable, data-protection-based objection.

5.3 The Processor will impose materially equivalent data-protection obligations on each sub-processor by written contract and remains responsible to the Controller for the sub-processor's performance of those obligations.

5.4 If the parties cannot reasonably resolve a Controller objection to a new sub-processor, either party may terminate the affected service in accordance with the Main Agreement.

6. Individual Rights

6.1 Taking account of the nature of the processing, the Processor will provide reasonable assistance through appropriate technical and organisational measures so that the Controller can respond to requests to exercise data-subject rights.

6.2 If the Processor receives a request relating to Controller personal data directly from an individual, it will not respond substantively except on the Controller's instructions or where required by law. It will refer the request to the Controller without undue delay where the Controller can be identified.

7. Compliance Assistance and Personal-Data Breaches

7.1 Taking account of the nature of processing and information available to it, the Processor will reasonably assist the Controller with security obligations, personal-data-breach assessment and notification, data-protection impact assessments and prior consultation with a supervisory authority.

7.2 The Processor will notify the Controller without undue delay after becoming aware of a personal-data breach affecting Controller personal data. The notification will include the information reasonably available to the Processor that the Controller needs to meet its notification obligations. Information may be supplied in phases as it becomes available.

8. Return, Deletion and Retention

8.1 During the Main Agreement, the Processor will provide reasonable assistance with an agreed export of Controller data.

8.2 At the end of the service, the Controller may request return or deletion of its personal data. The Controller should request an export before termination or promptly afterwards. The Processor will complete the agreed export or deletion of production data no later than 30 days after termination or receipt of a verified written deletion instruction. If no export is requested before production deletion is completed, the data may no longer be recoverable.

8.3 An export will be supplied as CSV or another reasonably agreed commonly used electronic format, taking account of the available service tools and the nature of the data.

8.4 The Controller acknowledges that deletion of historical organisation data also removes the history used for athlete metrics and cannot be reversed.

8.5 The production Supabase project is on the Pro Plan and uses daily database backups retained for seven days. Point-in-Time Recovery is not enabled. Deleted database records may therefore remain in a restricted daily backup for up to seven days after production deletion. Supabase database backups do not include files stored through its Storage API. If a backup is restored, applicable deletion instructions will be reapplied.

8.6 PowerSync is currently used on its Free Plan. Active synchronised service data will be removed within the production-data period in clause 8.2. PowerSync does not publish a fixed maximum period for residual archival or backup copies under this plan; any such copies remain subject to PowerSync's DPA and internal deletion practices, are not used for ordinary service delivery, and remain protected until overwritten or deleted. The Processor will provide updated supplier information to the Controller on reasonable request.

8.7 On an authorised user's device, the PowerSync offline cache may remain during connectivity loss or app force-close. After explicit logout, the cache may remain for up to 48 hours to permit same-user recovery of unsynchronised work. It is cleared when a different user signs in or when the app next initialises PowerSync after the 48-hour period.

8.8 Further storage is permitted only where required by UK law. Data retained for that reason will remain protected and will be processed only for the applicable legal purpose.

9. International Transfers

9.1 The Processor will not make a restricted transfer of Controller personal data except on documented instructions and using a lawful transfer mechanism.

9.2 Where the destination is not covered by UK adequacy regulations, the parties will use an appropriate safeguard, which may include the UK International Data Transfer Agreement or the UK Addendum to the European Commission Standard Contractual Clauses, together with the required transfer risk assessment or data-protection test and supplementary measures.

9.3 Relevant hosting and support locations and transfer safeguards are listed in Schedule 3.

10. Information and Audits

10.1 The Processor will provide information reasonably necessary to demonstrate compliance with this DPA and applicable processor obligations.

10.2 On reasonable written notice, the Processor will allow and contribute to an audit or inspection by the Controller or its independent auditor. Audits must avoid unnecessary disruption, protect other customers' confidentiality, and use available independent supplier reports and documentary evidence first where reasonable. Unless required following a breach or by a supervisory authority, the Controller will bear its audit costs.

10.3 The Processor will promptly inform the Controller if, in its opinion, an instruction infringes applicable data-protection law.

11. Liability, Priority and Law

- 11.1** Liability under this DPA is subject to the liability provisions in the Main Agreement except to the extent applicable law does not permit that limitation.
- 11.2** If this DPA conflicts with the Main Agreement on the protection of personal data, this DPA takes priority to the extent of the conflict.
- 11.3** This DPA is governed by the law and jurisdiction specified in the Main Agreement. If the Main Agreement does not specify them, the laws of England and Wales apply and the courts of England and Wales have jurisdiction.

Schedule 1 — Processing Details

Subject matter	Provision of the Impact Netball Club team, fixture, offline game-recording, synchronisation, statistics and reporting service.
Duration	For the term of the Main Agreement plus the return/deletion and protected backup-overwrite periods described in clause 8.
Nature and purpose	Collection from authorised users; hosting; organisation-based access; local offline caching; synchronisation; retrieval; calculation and display of performance statistics; report generation; support; security; backup; export and deletion.
Personal-data types	User email and access permissions; organisation, team and squad information; athlete name or identifier and team membership; fixture, opponent, location, date and time; game events; performance metrics and statistics; uploaded logos, team sheets or images; relevant technical, authentication, synchronisation and security records.
Data-subject categories	Athletes, including child athletes; coaches; school or club staff and administrators; other authorised users.
Special-category data	Not intentionally required or authorised unless the parties expressly agree additional instructions, lawful basis and safeguards in writing.
Frequency	Continuous or ad hoc as authorised users use the service.

Schedule 2 — Technical and Organisational Measures

- Supabase Row Level Security on service tables and organisation-based access rules.
- Authenticated access and assigned user roles and permissions.
- Separate permission checks for each school or club, including where one user is authorised for multiple organisations.
- TLS-protected cloud connections and cloud-provider encryption at rest.
- iOS secure credential storage for credentials saved through the optional remember-me feature.
- PowerSync offline operation with different-user clearing and a 48-hour post-logout retention rule.
- Restricted administrative access on a need-to-use basis.
- Software and dependency maintenance and release testing.
- Cloud backup and recovery arrangements described in clause 8.
- Incident investigation, containment and communication procedures.
- User-selected destinations for exported PDF reports; exported copies then fall under the Controller's and user's controls.

Supabase reports SOC 2 Type 2 compliance and ISO 27001 certification. PowerSync reports an independently audited SOC 2 Type 2 programme. These are supplier assurances and are not certifications held directly by Pegasus Sports Media.

Schedule 3 — Sub-processors and Locations

Provider	Service and data	Location	Safeguard
Supabase, Inc.	Database, authentication, storage and Edge Functions; application data and account identifiers.	Primary project data: AWS eu-west-2, West Europe (London), United Kingdom. Support and ancillary locations are governed by the Supabase DPA and sub-processor list.	Supabase DPA; UK adequacy where applicable; otherwise the UK Addendum or another appropriate safeguard.
Journey Mobile, Inc. / PowerSync	Synchronisation service and synchronised application data.	European Union service region. Supporting and administrative sub-processors may operate elsewhere as identified by PowerSync.	UK adequacy for applicable EEA processing; PowerSync DPA and the UK Addendum or another appropriate safeguard for restricted transfers.

Other service providers and recipients: SMTP2GO processes transactional account-administration emails in its configured European Union region. GoCardless processes subscription-payment data as an independent controller under its own privacy terms. Neither service receives school-controlled athlete or game content as part of its ordinary role.

Signatures

This standard DPA may be executed in counterparts and by electronic signature. A customer may request a signature-ready copy from impactnetball@pegasus-sports-media.com.

For the Controller Organisation: Name: Title: Signature: Date: 	For Pegasus Sports Media Limited Name: Title: Signature: Date:
---	--