

Data Protection and Children's Privacy Policy

Dragon Academy Ltd (company number 16871720)

Version 1.0 · Approved by Dylan Powell, Director · Designated Safeguarding Lead: Dylan Powell · Next review: by 31 October 2027

1. Purpose

Dragon Academy holds personal information about children, their parents and carers, and our coaches. Children's information needs particular care. This policy explains how Dragon meets the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, and how we protect children's information in particular.

The Dragon Players app also has its own privacy policy.

2. Who is responsible

- **Data controller:** Dragon Academy Ltd.
- **Data protection lead:** Dylan Powell, dylan@dragondevelopment.co.uk.
- **Regulator:** the Information Commission (formerly the Information Commissioner's Office, ICO; renamed on 30 September 2026). Its website is still ico.org.uk.
- **ICO registration:** Dragon Academy Ltd is registered with the Information Commission (ICO) and pays the annual data protection fee.

3. Our principles

We will:

1. use personal information lawfully, fairly and openly;
2. collect it only for clear purposes and not use it for anything else;
3. collect only what we need;
4. keep it accurate and up to date;
5. keep it only as long as we need it (section 9);
6. keep it secure (section 8); and
7. be able to show how we follow these principles.

4. What we hold

About	What	Notes
Children	Name, date of birth or age group, area and session, attendance, assessments and awards, app activity, photos and video (with consent)	
Children: health and needs	Medical conditions, allergies, medication, disabilities and additional needs that coaches need to know	Special category data
Children: safeguarding	Records of concerns, referrals and what was done	Highly sensitive. Seen only by the DSL and Deputy DSL
Parents and carers	Name, contact details, emergency contacts, who may collect the child, membership and payment records, messages	Card details are held by Dragon's payment providers, not by Dragon
Coaches	Contact details, agreement, qualifications, training, references, self-declaration, DBS check record, invoices	DBS and self-declaration information is criminal offence data

5. Why we use it, and the lawful basis

Purpose	Lawful basis (UK GDPR Article 6)
Running memberships, sessions, trials and events	Contract with the parent
Taking payments and keeping accounts	Contract; legal obligation (tax records)
Keeping children safe at sessions, registers, collection arrangements, accident records	Legitimate interests; legal obligation
Sharing information with the police, local authority or other agencies to protect a child	Legal obligation, or the recognised legitimate interest for safeguarding under the Data (Use and Access) Act 2025, or vital interests in an emergency
Photos and video, marketing emails and the Dragon Weekly newsletter	Consent (see policy 04). Marketing emails to existing families may instead rely on the "soft opt-in", with an easy way to unsubscribe
Vetting coaches	Legal obligation and legitimate interests

Health information is used with the parent's explicit consent, or without it where needed to protect a child's vital interests in an emergency.

Safeguarding information may be recorded and shared without consent where that is needed to protect a child, under the safeguarding condition in Schedule 1 to the Data Protection Act 2018.

Criminal offence data (DBS checks and self-declarations) is used only for vetting, under the conditions in Schedule 1 to the Data Protection Act 2018. Dragon keeps an appropriate policy document where the law requires one. **[To confirm with the solicitor or the ICO helpline.]**

6. Children's rights and consent

1. Children have the same data protection rights as adults. For younger children, a parent or carer normally exercises those rights for them.
2. Older children who understand what they are asking can make requests about their own information. The ICO says age 12 is typically given as a guideline. We consider each child's maturity and best interests, and listen to their views.
3. Children have a strong right to have information collected about them while they were children erased, and this continues after they turn 18. Dragon makes erasure as easy to ask for as it was to give the information.
4. Where we rely on consent (for example photos), we ask the parent, and we also respect a child who says no.
5. We never sell children's information, and we never use it for third-party advertising or profiling.

7. Sharing information

1. **Service providers.** We use carefully chosen service providers to run Dragon: website and bookings, payments, the Dragon Players app and its hosting, email and storage, text messages, and the newsletter. Each one processes information only on Dragon's instructions, under a contract that meets UK GDPR.
2. **Safeguarding.** Data protection law does not stop us sharing information to keep a child safe. Where a child may be at risk, we share what is necessary, accurate and relevant with the local authority or the police, and record what we shared, with whom, when and why.
3. **Never shared with sponsors or partners.** Sponsors, partner clubs and advertisers never receive children's or families' personal information.
4. **AI tools.** Children's personal information, images and any safeguarding information must not be put into AI tools, except tools that Dragon has approved in writing, under a contract with the provider, for a defined purpose that families have been told about (such as the Dragon Players app's "My AI Coach"). Safeguarding records are never put into AI tools.

8. Keeping information secure

1. Every person has their own login for every Dragon system. Logins are never shared.
2. Each person sees only what they need for their role. Coaches see the children in the groups they coach. Safeguarding records are seen only by the DSL and Deputy DSL.
3. Strong passwords and two-step verification are used wherever a system offers them.
4. Dragon information is not stored on personal devices or personal accounts. Devices used for Dragon have a screen lock and are kept up to date.
5. When someone leaves, or is suspended, their access to every Dragon system is removed **the same day**, and existing sessions are ended.
6. Paper records are kept to a minimum, in a locked place, and shredded when no longer needed.

9. How long we keep information

Record	How long	Basis
Membership and contact records	While the child is a member, then 2 years	Dragon's rule
Financial and payment records	6 years after the end of the financial year	Tax records
Accident and injury records about a child	Until the child is 25	Dragon's rule, in line with the safeguarding records period
Safeguarding records about a child	Until the child is 25, or longer if needed for legal proceedings or an official inquiry	NSPCC guidance, following the education sector rule in Wales
Records of allegations or concerns about an adult	Until the person reaches normal pension age, or for 10 years, whichever is longer, even if they stop working with Dragon	NSPCC guidance, following the education sector rule in Wales
DBS certificate information	Only as long as needed for the decision, and no more than 6 months. A record of the check (name, date of issue, type, position, certificate number and decision) is kept for the coach's time with Dragon plus 6 years	GOV.UK guidance on handling DBS certificate information; Dragon's rule
Coach agreements and vetting register	The coach's time with Dragon plus 6 years	Dragon's rule
Unsuccessful applicants	6 months	Dragon's rule
Photos and video	While consent lasts. Removed within 2 working days of a request	Policy 04
Consent records	While the image or consent is in use, plus 12 months	Dragon's rule

Records needed for a police investigation, legal claim or official inquiry are kept until it ends, whatever this table says.

10. If something goes wrong (data breaches)

1. Anyone who finds that personal information has been lost, stolen, sent to the wrong person, seen by someone who should not see it, or changed without permission, tells Dylan **the same day**.
2. Dylan records every breach, decides what to do to limit the harm, and decides whether to report it.
3. If the breach is likely to put people at risk, Dragon reports it to the Information Commission **within 72 hours** of becoming aware of it.
4. If it is likely to put people at high risk, Dragon tells the people affected without delay.

11. Requests from families and coaches

1. Anyone can ask for a copy of their information, or ask us to correct, delete, restrict or stop using it. Requests can be made in any form, but email to dylan@dragondevelopment.co.uk is easiest.
2. Dragon responds within **one month**. There is normally no charge.
3. We check the identity of the person asking, and, for a child's information, that they have parental responsibility or the child's authority.
4. Some information may be withheld where the law allows, for example where releasing it would put a child at risk or would identify someone who raised a safeguarding concern.

12. Complaints

1. Since 19 June 2026 the law requires every organisation to have a process for data protection complaints. Complaints about how Dragon uses personal information go to Dylan Powell. People can complain by email to dylan@dragondevelopment.co.uk or in writing.
2. Dragon acknowledges a complaint within 30 days, looks into it, and tells the person the outcome without undue delay.
3. Anyone can also complain to the Information Commission: ico.org.uk, 0303 123 1113.

13. The Dragon Players app

The Dragon Players app is used by parents, coaches and, through linked player logins, by children. Dragon will:

1. complete a data protection impact assessment (DPIA) for the app and keep it up to date;
2. follow the ICO's Age Appropriate Design Code (the Children's code). The code covers apps that children are likely to use, not only apps aimed at children. Because the app has player logins and games for children, Dragon assumes it applies, unless the DPIA documents good reasons that it does not;
3. keep children's settings private by default and collect only what is needed;
4. make sure coaches' messages about a child go to the parent, not to the child; and
5. keep the app's privacy policy accurate, including on photos.