



Privacy Policy

Flair Elite Ltd · Flair Elite App

Version: 1.0

Effective date: 10 October 2026

Last updated: 10 October 2026

Website: flairelite.app

Your privacy, in plain English

Flair helps you turn your sporting experience into skills, learning opportunities and career options. This policy explains what personal information we use, why we use it, who can receive it and how you can stay in control.

If you are aged 14–17, start here

- You have rights over your information. You can ask us what we hold, correct something that is wrong or ask us to delete information.
- Your employment status, Jobcentre referral and private support information are not included in employer-facing profiles by default. Your academy background is not made public simply because you tell us about it.
- Optional sharing of your Skills Passport is a separate choice. We explain what will be shared and who will receive it before you choose.
- You do not have to agree to optional marketing to use Flair. You can say no to optional information requests.
- Career suggestions and match scores are suggestions, not a judgement of your worth or a promise of a job.
- If anything is confusing or worries you, email Stacey@flairelite.com or becky@flairelite.com. You can ask a trusted adult to help you. Being your parent or carer does not automatically give someone access to your account.

1. Who is responsible for your information?

Flair Elite Ltd is the **data controller** for personal information used to operate the Flair Elite App at flairelite.app. This means we decide why and how that information is used.

Our privacy contacts are:

Email: Stacey@flairelite.com or becky@flairelite.com

Postal address:

Privacy enquiries — Flair Elite Ltd

139 Boot Hill

Atherstone

CV9 2EW

United Kingdom

You may contact either email address. You do not need to send your enquiry to both.

This policy covers individual members, including members aged 14–17, and personal information about employer and education or training-provider representatives who use the app. We handle personal information in accordance with applicable UK data protection law, including the UK GDPR and the Data Protection Act 2018, as amended.

An employer, academy, training provider or referral organisation may be independently responsible for information it holds. Its own privacy notice applies to that separate use of information.

2. Who can use Flair?

Flair is available to users **aged 14 and over**. It is not intended for children under 14.

We use the minimum age information needed to establish eligibility and apply appropriate account protections. Any additional age or identity check will be explained at the point it is requested, including the information needed and how it will be handled. We do not make your age-verification information public.

If we learn that an account belongs to someone under 14, we will stop their use of the account, investigate and remove information we do not have a lawful reason to retain. Any necessary safeguarding or legal record will be limited and access-restricted.

People aged 14–17 have their own privacy rights. We give particular consideration to their best interests when deciding what to collect, how to explain it and whether to share it. We apply high-privacy settings by default and provide age-appropriate explanations. We do not use

prompts that pressure children to disclose unnecessary information or weaken their privacy settings.

Any request for consent must be understandable to the person making the choice. Additional support or checks may be needed for particular activities; this does not mean every account automatically requires parental consent.

3. What information do we collect?

The information we collect depends on the features you use.

Account and contact information

This includes your name, email address, account type, age information where needed, login identifiers and records of your privacy choices. If you choose a third-party sign-in option, we receive the identity and account information you authorise that provider to share. We also hold records needed to manage your account.

Sporting, academy and skills information

This can include your sport, sporting background, academy history, club or association, experience, profile description, skills ratings and evidence used to build or verify your Skills Passport. The app also creates information such as skill summaries and match results from the information used by the relevant feature.

Employment and referral information

This includes the employment status you provide, whether you were referred through the Department for Work and Pensions (**DWP**) or Jobcentre, and information needed for a specific support or funded programme where applicable.

A referral flag is not permission to collect your complete benefits record. Please do not upload benefit statements, National Insurance numbers, medical records or other detailed documents unless we have separately explained why a particular document is necessary and how it will be handled.

Applications and participation

Where you use the relevant features, we collect the information you submit in a job or course application, application status, enrolment or verification records, and communications about your participation.

Organisation representatives

For employer and educator or training-provider accounts, we collect contact and work-role details, organisation information and records of activity carried out through the account. Business information can also be personal information when it identifies an individual.

Technical information and communications

We collect technical information needed to operate and protect the app, such as connection or security logs and device or browser information. We also keep messages you send us and records of support, privacy requests and complaints. Cookies and similar technologies are addressed in section 11.

Health and other particularly protected information

Employment status, a simple DWP referral flag and academy background are personal information, but they are **not automatically special-category data** under UK data protection law. An injury description, disability information or the reason for a particular referral may reveal health information and require additional protection.

Please do not put medical details, ethnicity, religious beliefs, trade union membership or other particularly protected information into a general profile or free-text answer. If we need such information for a specific purpose, we will explain that purpose, the additional legal condition, who can see it and whether providing it is optional before collecting it.

Criminal offence information is subject to separate rules. It should not be submitted unless we have specifically requested it through an appropriate process.

4. Where does your information come from?

Most information comes from you when you register, complete your profile, rate skills, use a feature or contact us. Some is created by the app, such as account activity and match results.

Where you connect or participate through another organisation, information may come from your academy, club, educator, training provider, employer, DWP or an authorised referral partner. This could include confirmation of experience, enrolment, qualifications or a referral. We identify the relevant source and information in the notice for that connection or programme.

If information is supplied by someone else, we provide the required privacy information within the applicable legal timescale. This will normally be within one month, and earlier where required because we first contact you or disclose the information. Any applicable exception is considered separately; a referral does not remove our transparency duties.

5. Why do we use information, and what is our legal basis?

We need a lawful basis for each use of personal information. The bases for the activities described in this policy are set out below.

Providing your account, profile and Skills Passport

We use account, sporting and skills information to run the service you request, support your account and maintain your Skills Passport. Our basis is **legitimate interests — Article 6(1)(f)**: providing a useful sporting-to-career service and responding to members' requests. We assess whether the use is necessary and fair, giving particular weight to children's rights and reasonable expectations.

Providing relevant learning and career suggestions

We use the profile, skills and preferences relevant to the feature to suggest opportunities. Our basis is **legitimate interests — Article 6(1)(f)**: helping members find relevant opportunities. Optional profiling for users under 18 is subject to the safeguards in section 7 and is not enabled merely because an account has been created.

Delivering referral or programme support

Where relevant, we use the minimum employment and referral information necessary to identify and deliver the support you request. Our basis is **legitimate interests — Article 6(1)(f)** for requested support. A funded programme may have a different, separately documented basis and notice. We explain any programme-specific reporting before participation. A commercial funding agreement does not, by itself, establish a legal obligation to process your information.

Applications and requested disclosures

We use the information needed to administer the job or course application, enrolment or verification activity you request. Our basis is **legitimate interests — Article 6(1)(f)**: helping you pursue an opportunity or verify your experience. We explain the recipient and information involved before disclosure. The recipient is responsible for establishing its own basis for its subsequent use of that information.

Optional sharing and marketing

For genuinely optional, separate choices to share your profile beyond necessary service delivery or receive marketing, our basis is **consent — Article 6(1)(a)**. Refusing or withdrawing these choices does not remove your access to unrelated core features. We do not treat acceptance of this policy as consent to optional processing.

Security, support and service administration

We use relevant account, technical and communication information to prevent misuse, investigate faults and respond to requests. Our basis is **legitimate interests — Article 6(1)(f)**: maintaining a secure, reliable service and resolving user concerns. Optional tracking is not justified simply by describing it as security or service improvement.

Meeting specific legal duties

Where a particular law requires us to retain or disclose information or handle a request or complaint, we rely on **legal obligation — Article 6(1)(c)**. This includes applicable data protection duties concerning rights requests and complaints. We identify the relevant requirement rather than treating every business need as a legal duty.

If special-category information is processed, we also need an applicable **Article 9 condition**, in addition to the Article 6 basis. For genuinely optional health or support information, this may be explicit consent. We explain the applicable condition before collecting the information and do not assume consent is valid where you do not have a real choice. Other conditions require their own justification and, where applicable, statutory safeguards.

6. Who can receive your information?

Flair staff and service providers

Authorised staff receive access where needed for their role. We use service providers for functions such as app hosting and delivery, account authentication, database and backup storage, service communications, and technical support. Where they process information on our behalf, they do so under appropriate contractual instructions and safeguards. Their access is limited to what is needed for the service they provide.

Third-party sign-in providers process information under their own notices as well as supplying the account information you authorise them to share with us. You can ask our privacy contacts for more information about relevant providers and their roles.

Employers, educators and training providers

A recipient may receive the information needed for an application, course enrolment, skills verification or sharing action that you choose. Before disclosure, we explain the recipient and relevant information. The recipient may then use that information under its own privacy notice.

Your profile is not publicly searchable by default. Optional employer discovery is off for users under 18. A private Skills Passport or direct application is different from making a profile available to all employers. Employment status, DWP referral and private support information are excluded from employer-facing views unless a specific, justified disclosure has been explained.

DWP, Jobcentre, referral partners and funders

A self-declared DWP referral does not give DWP unrestricted access to your profile. If a programme requires identifiable attendance, progress or outcome reporting, its notice specifies what is reported, to whom, why and under which basis. Where genuinely anonymous reporting is sufficient, we do not supply identifiable information for that reporting.

Legal and safeguarding disclosures

Information may be disclosed where required by law or where a specific lawful and proportionate disclosure is necessary to protect someone or address a serious incident. We limit the information and document the reason. A safeguarding concern is not a general licence to share all account information.

We do not sell personal information or use private employment, referral or health information for behavioural advertising.

7. Matching, profiling and automated decisions

Flair's matching features use information such as your skill ratings and relevant profile details to compare your experience with opportunity requirements. They may generate scores, identify gaps and suggest learning or career options. This is a form of **profiling** when personal information is used to evaluate aspects of your skills or suitability.

A match score can be incomplete or wrong. It is not a guarantee of admission, employment or qualification. You can ask us to correct the information used and explain a result.

For users aged 14–17, profiling is off by default unless we have documented a compelling reason that it is in their best interests and implemented suitable protections. Where an optional recommendation feature is offered, we explain its use and controls in age-appropriate language before activation.

We do **not** make solely automated decisions with legal or similarly significant effects, such as automatically refusing someone access to a funded programme or deciding whether an employer hires them. Employers and training providers remain responsible for their own decisions and privacy practices.

If a new feature changes how we evaluate your information or introduces significant automated decision-making, we will explain the processing and applicable safeguards before using it.

8. Is providing information compulsory?

Some information is necessary for a particular feature. For example, an email address is needed to establish an email-based account, and relevant skills information is needed to produce meaningful skills-based suggestions. If you do not provide necessary information, we may not be able to provide that feature.

We identify required and optional fields when asking for information. Academy history, employment status and DWP referral are not universally required merely because they may be relevant to a particular programme. Where an answer is optional, you can decline to provide it without losing access to unrelated features.

If a specific programme requires information under a law or a valid contractual condition, we explain the requirement and consequences before collecting it. Choosing not to provide optional information or consent may limit the optional activity concerned, but does not prevent unrelated use of Flair.

9. How long do we keep information?

We retain information only for as long as it is needed for the purpose for which it was collected, or for a separately justified legal requirement. We assess retention by category rather than keeping an entire account indefinitely. The following criteria determine retention:

- **Account and Skills Passport records:** while you use the service, followed only by any justified period needed to handle closure, outstanding requests or a dispute. We review inactive accounts rather than keeping them indefinitely.
- **Employment, referral and programme records:** while needed to deliver relevant support and for any documented reporting or audit period that applies to the programme. These records do not remain in general profiles merely because an account stays open.
- **Applications and verification records:** for the relevant application or verification process and any explained follow-up, dispute or programme requirement.

- **Age and identity-check information:** only for the time needed to carry out and evidence the relevant eligibility or identity check. We limit any longer-term record to what is necessary for that purpose.
- **Security logs and technical records:** for a limited period proportionate to detecting misuse, investigating incidents and keeping the service reliable.
- **Privacy choices, requests and complaints:** for the period needed to act on the request and demonstrate that it was handled correctly. A minimal suppression record may be needed to respect a marketing opt-out.

We delete or genuinely anonymise information when it is no longer needed. Account closure does not always require immediate deletion of every record, but any record retained must have a specific reason and restricted use.

Information removed from active systems may remain in restricted backups until those backups expire through their retention cycle. It is not used for routine processing. If a backup is restored, deletion instructions must be reapplied. You can contact us for the retention arrangements applicable to your information or programme.

Recipients acting as separate controllers manage their own retention under their privacy notices.

10. How do we protect information, and is it sent abroad?

We use appropriate technical and organisational measures for the nature and risks of the information, including role-based access and controlled handling of private records. No system can be guaranteed completely secure.

Our service providers may store or access information outside the UK. Where this is a restricted international transfer, we use an applicable UK adequacy arrangement or another lawful transfer mechanism, with the necessary assessments and additional protections where required. Relevant mechanisms may include the UK International Data Transfer Agreement or the UK Addendum to EU standard contractual clauses.

You can ask our privacy contacts for information about the locations and recipients relevant to your information, and for a copy or description of the applicable transfer safeguards. We may redact information where necessary to protect confidential information without preventing you from understanding the safeguards.

11. Cookies, local storage and similar technologies

The app uses cookies, local storage and similar technologies where needed to maintain sign-in, remember necessary preferences and operate its features.

Any optional analytics, advertising or other tracking is separately identified and explained at the point of use, including its provider, purpose and duration. Where consent is legally required, optional technology is not activated before a valid choice. Refusing it is a real option, and we explain how to change any choice. A privacy-policy acknowledgement does not provide cookie consent.

If a current legal exemption applies to a technology, we still explain the use and provide any required control. Browser or device settings may also let you manage storage; blocking essential technologies may prevent some features from working.

We do not use children's information for behavioural advertising. Under-18 privacy settings are not weakened through prompts that pressure people to disclose more information.

12. Your rights and how to use them

Depending on the processing and applicable exceptions, you can:

- Ask for access to your personal information and a copy of it.
- Ask us to correct inaccurate or incomplete information.
- Ask us to delete information where the right to erasure applies.
- Ask us to restrict particular uses of your information.
- Request portability of information where the processing is automated and based on consent or a contract.
- Withdraw consent for processing that depends on consent. Withdrawal does not make earlier lawful processing unlawful, but we must stop the relevant consent-based processing unless another properly established basis applies.
- Exercise applicable safeguards concerning significant automated decisions.

Your right to object

You can object to processing based on legitimate interests because of your particular circumstances. We must consider your objection and stop unless we can demonstrate an applicable overriding justification or another legal exception. You can object to direct marketing at any time, and we will stop that marketing.

To use a right, email either Stacey@flairelite.com or becky@flairelite.com, or write to the address in section 1. Explain what you want us to do and identify the relevant account. Do not send identity documents unless we reasonably request them through an appropriate channel.

If processing relies on consent, you can withdraw it through the control provided for that choice or by contacting us. Withdrawal is as easy as giving consent and does not affect unrelated core features.

We may ask for proportionate information to check identity or clarify a request where permitted. We normally respond to rights requests within one calendar month, subject to the applicable rules on identity checks, clarification and extensions. If we need more time or cannot fulfil a request, we explain why and your options. Requests are normally free of charge.

Children have these rights too. A parent, carer or other representative can help, but we consider the young person's understanding, wishes, authority and circumstances before sharing information or acting on their behalf. We do not grant automatic parental access merely because a member is under 18.

13. Questions and complaints

If you are concerned about how we handle information, contact either privacy email address or the postal address in section 1. You may use the subject line **“Privacy complaint”**, but a particular wording or form is not required.

We will acknowledge a data protection complaint within **30 days**, investigate it appropriately, keep you informed as appropriate and communicate the outcome without undue delay.

You also have the right to complain to the UK Information Commissioner’s Office (**ICO**). You do not lose this right by raising the matter with us.

ICO complaints: ico.org.uk/make-a-complaint

14. Changes to this policy

We will update this policy when the service or its information use changes and show the effective date and version at the top. We will explain material changes in an appropriate way, using clear wording for younger members. If a new purpose requires additional information or consent, we will provide the explanation and obtain any necessary consent before starting that use.

Using the app after a policy update does not, by itself, give consent to new optional processing.