



Enriching children's lives through practical learning and outdoor activities

Flourish at the Farm Privacy Notice

Version: V5.1 September 2026

Last reviewed: September 2026

Next scheduled review: September 2027

1. About this notice

This privacy notice explains how Flourish at the Farm collects, uses, stores and shares personal information about:

- children and young people who use our services;
- parents, carers and guardians;
- prospective participants and their families;
- school, local authority and professional contacts;
- website visitors and people who contact us; and
- other individuals whose personal information we handle in providing our services.

We recognise that children and young people merit particular protection. We aim to explain our use of their information in language appropriate to their age and understanding. A child-friendly version of this notice is available from us on request and should also be provided directly to children and young people where appropriate.

This notice applies to our alternative education provision, post-16 provision, HAF activities, educational and wellbeing programmes, enquiries, bookings, website and related services.

It should be read alongside any specific privacy information we provide when collecting information for a particular activity.

2. Who we are

Flourish at the Farm is the organisation responsible for deciding how and why personal information covered by this notice is used. This means that, except where another organisation is responsible, we are the *controller* of that information.

Our contact details are:

Flourish at the Farm

Kings Lane

Snitterfield

Stratford upon-Avon

CV37 0QA

Website: www.flourishatthefarm.co.uk

Email: admin@flourishatthefarm.co.uk

Telephone: 01789576600

Legal entity: Flourish at The Farm Ltd

Company number: 11990878

ICO registration number: ZB283897

Our person responsible for data protection is: Lead Admin Kim Price

Data Protection Lead: Lead Admin Kim Price

Email: admin@flourishatthefarm.co.uk

Flourish at the Farm has not appointed a statutory Data Protection Officer unless expressly stated otherwise. References in this notice to our Data Protection Lead mean the person who manages privacy matters for us.

3. When another organisation is responsible

Schools, colleges, local authorities, HAF programme organisers, health professionals and other referring bodies may send information to us. They will usually remain controllers of the information they hold for their own purposes. Depending on the service and contractual arrangements, Flourish at the Farm may act as:

- an independent controller;
- a joint controller with another organisation; or
- a processor acting on the documented instructions of a school, local authority or other commissioning body.

Where necessary, the relevant referral, placement or service documentation

will explain the arrangement. You may contact us if you are unsure which organisation is responsible for a particular use of information.

4. Information we collect

We collect only information reasonably required for our services and legal responsibilities. Depending on the relationship and service, this may include:

- names, preferred names, pronouns, dates of birth, age and gender;
- home, email and telephone contact details;
- parent, carer, guardian and emergency-contact details;
- family circumstances and the individual's relationship to the child;
- school, college, local authority, social worker and other professional details;
- referrals, education plans, attendance records, learning records, progress reports, assessments and qualifications;
- Education, Health and Care Plan information;
- special educational needs and disabilities information;
- physical and mental health information, allergies, medication, dietary needs, accidents, injuries and first-aid records;
- GP or other healthcare contact details where needed;
- behavioural, emotional, social, pastoral and wellbeing information;
- safeguarding and child-protection concerns, referrals, allegations and related records;
- race or ethnic origin, religion or belief, where relevant and lawful;
- care status and other information about vulnerability or support needs;
- accessibility and communication requirements;
- activities, sessions, camps or programmes attended;
- arrival, departure and authorised-collection information;
- correspondence, complaints, feedback, surveys and records of contact;
- photographs, video or audio recordings;
- billing, payment and transaction details, but not normally complete payment-card credentials where payments are handled by a payment provider;
- contractual, consent and permission records;
- website account or booking information;
- staff notes and incident records;
- CCTV recordings, if CCTV is in operation and appropriate signs are displayed;
- information necessary for security, fraud prevention and legal claims; and
- any other information supplied to us which is relevant to the service or

enquiry.

Website and device information

When someone uses our website or online services, we and our authorised suppliers may collect:

- IP address;
- browser, device and operating-system information;
- approximate location derived from an IP address;
- pages viewed and links selected;
- dates, times and duration of visits;
- referring website;
- form submissions and booking activity;
- cookie identifiers and consent choices; and
- diagnostic, security and performance information.

More detail should be provided in our separate Cookie Policy and through the website's cookie controls.

Criminal-offence information

Safeguarding records may sometimes contain information about alleged or proven criminal conduct. We use this information only where authorised by law, such as where necessary for safeguarding, regulatory or legal purposes. We apply appropriate access, security and retention controls.

5. Where we obtain information

We may receive information:

- directly from a child or young person;
- from a parent, carer, guardian or emergency contact;
- from schools, colleges and alternative provision settings;
- from local authorities and HAF programme organisers;
- from health, social care, SEND and safeguarding professionals;
- from police or other public bodies where lawful;
- from examination, accreditation or awarding organisations;
- from contractors and activity providers;
- from payment, booking and technology suppliers;
- through our website, forms, email, telephone and social-media accounts;
- from publicly available sources where appropriate; and
- from another person where needed to deal with an emergency, incident, complaint or legal matter.

Where information was not obtained directly from the person concerned, we normally provide privacy information within one month, at our first communication with them, or before the information is disclosed, unless a lawful exception applies.

6. Why we use information and our lawful bases

UK data protection law requires us to identify a lawful basis for each use of personal information. More than one basis may apply.

Purpose	Principal lawful basis
Responding to enquiries and arranging placements, programmes, activities or camps	Steps requested before entering a contract; contract; legitimate interests
Delivering education, alternative provision, post-16 support, camps and activities	Contract; legal obligation; legitimate interests; public task where applicable
Supporting learning, attendance, development, wellbeing and reintegration	Contract; legitimate interests; public task where applicable
Protecting children and others, managing safeguarding concerns and emergencies	Legal obligation; vital interests; legitimate interests; public task where applicable
Managing health, medication, allergies, accessibility and emergency care	Legal obligation; vital interests; contract; legitimate interests, together with an Article 9 condition
Communicating with families, schools, authorities and professionals	Contract; legal obligation; legitimate interests; public task where applicable
Maintaining records, reporting to commissioners and demonstrating delivery	Contract; legal obligation; legitimate interests; public task where applicable
Processing fees, payments and accounting records	Contract; legal obligation; legitimate interests
Managing incidents, complaints, disputes and legal claims	Legal obligation; legitimate interests
Ensuring safety, security and preventing fraud	Legal obligation; legitimate interests
Improving services, quality assurance and staff development	Legitimate interests; consent where required
Taking and using photographs or recordings	Consent where required; in limited operational contexts, legitimate interests
Sending marketing communications	Consent, or legitimate interests where permitted; electronic marketing is also

Purpose	Principal lawful basis subject to PECR
Operating, securing and improving our website	Legitimate interests; consent for non-essential cookies or similar technology
Complying with regulators, courts and public authorities	Legal obligation; public task where applicable

Contract

We use information when it is necessary to enter into or perform a contract with a parent, young adult, school, local authority or another commissioning body.

A child may not personally be a party to that contract. Where contract is not an available basis for using the child's information, we use another appropriate basis, such as legitimate interests, legal obligation, vital interests or public task.

Legitimate interests

Our legitimate interests include:

- providing safe, effective and appropriate education and activities;
- supporting learning, wellbeing and development;
- communicating with families, commissioners and professionals;
- operating and improving our organisation;
- protecting participants, staff, property and systems;
- recovering money owed to us; and
- establishing, exercising or defending legal claims.

Before relying on legitimate interests, we consider the necessity of the processing, its likely impact and the particular rights and interests of children.

We do not use this basis where those rights and interests override ours.

You may ask for information about a relevant legitimate-interests assessment.

Consent

Where we rely on consent, it must be freely given, specific, informed and capable of being withdrawn. Withdrawing consent does not make earlier processing unlawful.

For children, we consider the child's age, maturity and understanding and whether consent should be obtained from the child, a person with parental responsibility, or both. We do not treat parental consent as automatically replacing a competent child's data-protection rights.

Refusing or withdrawing optional consent will not affect access to the core service unless the relevant information is genuinely required to provide it safely.

7. Health, SEND and other special-category information

Health, disability, SEND, racial or ethnic origin, religion or belief, and certain other information receive additional legal protection.

In addition to an Article 6 lawful basis, we use an appropriate Article 9 condition. Depending on the circumstances, this may include:

- explicit consent;
- protection of someone's vital interests where that person cannot consent;
- health or social care and the management of relevant services;
- reasons of substantial public interest under the Data Protection Act 2018, including safeguarding children and individuals at risk;
- equality of opportunity or treatment, where the legal conditions are met; or
- establishing, exercising or defending legal claims.

Where a Data Protection Act 2018 condition requires it, we maintain an Appropriate Policy Document explaining our procedures and retention safeguards.

We limit access to this information to staff and authorised persons who need it. An essential allergy, medication or emergency-care summary may be made readily available to relevant staff where necessary to keep a participant safe. We do not rely on consent where consent is not genuinely optional or where another lawful basis is more appropriate, including many safeguarding situations.

8. Safeguarding and information sharing

The safety and welfare of children and young people are paramount. Data protection law does not prevent necessary and proportionate information sharing to protect a child or another person from harm.

We may record and share relevant information with:

- the child's school or education provider;
- local authority education, SEND, social-care or safeguarding teams;
- designated safeguarding leads;
- health professionals and emergency services;
- police and other law-enforcement bodies;
- the Disclosure and Barring Service;
- Ofsted or another regulator; and
- other organisations involved in protecting or supporting the child.

We do not normally seek consent where doing so could place someone at greater risk, prejudice an investigation or prevent us from fulfilling a safeguarding or legal duty. We share only information that is relevant and

proportionate, unless an emergency or legal requirement makes wider disclosure necessary. [ICO safeguarding guidance](#)

9. Who receives information

Where necessary and lawful, information may be shared with:

- parents, carers and guardians, taking account of the child's rights, competence, safety and family circumstances;
- referring schools, colleges and other education providers;
- local authorities, HAF organisers and commissioners;
- SEND, health, social-care and safeguarding professionals;
- emergency services, police, courts and public authorities;
- Ofsted, awarding organisations and relevant regulators;
- activity specialists and service partners;
- insurers, legal advisers, accountants, auditors and debt-recovery providers;
- website, email, cloud-storage, management-information, booking, communication and IT-support providers;
- payment processors and banks;
- survey, mailing and marketing providers where permitted;
- photographers or media providers, where appropriate permissions and safeguards are in place;
- prospective purchasers, investors or professional advisers in connection with a proposed organisational restructuring or sale, subject to confidentiality and legal safeguards; and
- any other recipient where disclosure is required by law or necessary to protect someone's vital interests.

Our service providers are permitted to use information only for authorised purposes and must protect it under contractual and legal duties.

We do not sell children's or families' personal information.

10. Photographs, video and audio

We will only take videos, audio recordings or photos of staff with their consent.

We do not take pictures, record audio or video of students.

Any photographs used in our marketing or website material will be of the site, activity without students (may include consenting staff) or stock images with licenses.

We distinguish between operational uses and optional publicity. We will obtain

appropriate consent from staff before using any images for optional external marketing. Consent may be withdrawn for future use, although it may not always be possible to retrieve material already printed, downloaded, reposted by others or otherwise outside our control.

11. Marketing

We may tell parents, carers and adult participants about similar services where the law permits. Electronic marketing by email, text or similar means is sent only where PECR permits it, such as where valid consent exists or the applicable existing-customer rule is satisfied.

We do not use children's information for behavioural advertising. We do not ordinarily send direct marketing to children.

Anyone may opt out at any time by:

- using the unsubscribe option in a message; or
- contacting us using the details in section 2.

We may retain a minimal suppression record after an opt-out to ensure we honour the preference.

Service communications, safeguarding messages and essential information about an existing placement or booking are not marketing.

12. Cookies and online services

Essential cookies and similar technologies may be used where necessary to operate and secure our website.

We will seek consent before placing or accessing non-essential cookies, including analytics or advertising cookies, unless a legal exemption applies. Users should be able to accept or reject non-essential cookies and change their choices later.

Our Cookie Policy should identify:

- each cookie or comparable technology;
- its provider;
- its purpose;
- its duration;
- whether information goes to another country; and
- how consent can be withdrawn.

Our website may link to third-party websites and social-media services. Those organisations are responsible for their own privacy practices. Selecting an external link may allow that organisation to collect information under its own notice.

If we introduce an online service likely to be accessed by children, we will assess whether the Children's Code applies and implement age-appropriate

privacy information and protections. [ICO children's guidance](#)

13. International transfers

Some technology or service providers may process information outside the United Kingdom.

Before making a restricted international transfer, we use an appropriate legal mechanism, such as:

- UK adequacy regulations;
- the UK International Data Transfer Agreement;
- the UK Addendum to the EU Standard Contractual Clauses; or
- another exception or safeguard permitted by law.

Where required, we carry out a transfer risk assessment and apply supplementary security measures. You may contact us for information about the relevant safeguard and how to obtain a copy, subject to lawful redactions. Before publication, Flourish must identify its actual overseas providers and transfer mechanisms here or in a linked supplier schedule.

14. How long we keep information

We keep information only for as long as necessary for the relevant purpose, taking account of:

- legal, education, safeguarding and regulatory requirements;
- applicable limitation periods;
- the age of the child;
- contractual and insurance requirements;
- the nature and sensitivity of the information;
- the risk of harm from unauthorised use or disclosure; and
- whether the purpose can be achieved using less information.

Our detailed retention schedule governs individual record types. Typical periods are:

Record category	Indicative retention approach
Enquiries that do not become a placement or booking	12 months
Core participant, placement, attendance and progress records	7 years
SEND and health information	For the service period and then according to the education, safeguarding, limitation and insurance requirements that apply

Record category	Indicative retention approach
Child-protection and safeguarding records	Kept separately and retained according to applicable safeguarding guidance, contractual requirements and legal limitation periods; not subject to an automatic age-15 deletion rule
Accident and first-aid records	7 years
Complaints and disputes	7 years
Financial and tax records	Normally six years after the end of the relevant accounting period, or longer if required by law
Marketing consent and opt-out records	While marketing continues, plus sufficient evidence of consent or objection afterwards
Recruitment and DBS-related records	Under the separate workforce privacy notice and retention schedule
CCTV, if used	n/a
Website security logs and analytics	As specified in the Cookie Policy and supplier schedule

Information may be retained longer where an incident, safeguarding concern, complaint, claim, inquiry or legal requirement makes that necessary.

When the retention period ends, information is securely deleted, destroyed or irreversibly anonymised. The previous policy's blanket promise to delete a child's record shortly after age 15 has been removed because it may conflict with safeguarding, education, insurance and legal requirements.

15. Security

We use proportionate technical and organisational safeguards, which may include:

- role-based access and confidentiality obligations;
- staff training and safeguarding procedures;
- secure accounts, passwords and multi-factor authentication where available;
- encryption in transit and, where appropriate, at rest;
- secure storage and disposal;
- backups, malware protection and software updates;
- supplier checks and data-processing agreements;
- procedures for incidents and personal-data breaches; and
- periodic review of access, systems and policies.

No internet transmission or storage system is completely secure. We nevertheless remain responsible for applying appropriate safeguards and for

responding to incidents in accordance with the law.

Where a personal-data breach is likely to risk people's rights and freedoms, we will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the breach is likely to create a high risk, we will also notify affected individuals without undue delay unless a lawful exception applies.

16. Automated decisions and profiling

We do not currently intend to make decisions about children or families based solely on automated processing where those decisions produce legal or similarly significant effects.

Technology may assist with administration, assessment or service delivery, but significant decisions should involve meaningful human judgement.

If this changes, we will provide information about:

- the decision and the information used;
- the logic and likely consequences;
- the legal basis;
- the safeguards in place; and
- the rights to obtain human intervention, express a view and challenge the decision.

17. Your rights

Data-protection rights belong to the individual whose information is being used, including a child. A parent or person with parental responsibility may exercise a child's rights where authorised and appropriate, but this depends on the child's age, competence, circumstances and best interests.

Subject to legal conditions and exceptions, an individual may have the right to:

- receive information about how their information is used;
- obtain confirmation that we use their information and receive a copy;
- have inaccurate information corrected and incomplete information completed;
- have information erased;
- restrict how information is used;
- object to processing based on legitimate interests or public task;
- object at any time to direct marketing;
- receive and transfer certain information in a portable format;
- withdraw consent at any time where processing depends on consent;
- obtain safeguards relating to solely automated significant decisions; and
- complain about our use of personal information.

Not every right applies in every situation. For example, we may need to retain

information for safeguarding, legal claims or compliance with a legal duty. To exercise a right, contact our Data Protection Lead using section 2. Please describe the information or processing concerned. You do not have to use a particular form.

We may request reasonable evidence of identity and authority. We will not request more information than necessary. The usual response period is one month, beginning when we have received the request and any reasonably required identity information or permitted fee. The law allows an extension in certain circumstances, and we will explain if one applies.

We normally do not charge a fee. A reasonable fee may be charged, or a request refused, where the law permits this because it is manifestly unfounded or excessive.

A child's right of access does not automatically give a parent unrestricted access to all of the child's records. We consider confidentiality, competence, safeguarding, court orders and the rights of other people before disclosing information.

18. Data-protection complaints

You may make a data-protection complaint by writing to the Data Protection Lead using the contact details in section 2. Please state that you are making a data-protection complaint and provide enough information for us to understand and investigate it.

We will:

- provide a clear means of making the complaint;
- acknowledge it within 30 days of receipt;
- take appropriate steps to investigate it without undue delay;
- keep you informed where appropriate; and
- tell you the outcome without undue delay.

These complaint-handling duties have applied to organisations since 19 June 2026 under the Data (Use and Access) Act 2025. [ICO complaint guidance](#)

You may also complain to the Information Commissioner's Office. We would welcome the opportunity to address the issue first, but you are not required to surrender your right to approach the ICO.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

The current complaint route is available on the [ICO website](#).

19. Providing information to us

Some information is optional. Other information is needed to:

- enter into or perform a contract;
- meet a legal or safeguarding requirement;
- arrange funding or a placement; or
- provide a service safely.

If required information is not provided, we may be unable to accept a referral, deliver a service, administer medication, meet a particular need or permit participation in an activity. We will explain the likely consequence at the time.

20. Changes to this notice

We review this notice regularly and whenever our services, systems, suppliers or legal obligations change.

The current version will be published on our website. Where a change is significant, we will take reasonable steps to bring it to the attention of affected people before the new use begins. Earlier versions may be requested from us.

Child-friendly summary

Flourish at the Farm uses information about you so that we can teach you, support you and keep you safe.

We may know things such as your name, age, school, support needs, health information and how you are getting on. We may receive this from you, your parent or carer, your school, the local authority or another professional helping you.

We share information only when there is a proper reason. This might be with your school, parent or carer, support professionals, or someone who needs the information to help protect you. If we are worried that you or someone else is unsafe, we may need to share information without asking first.

You can ask us:

- what information we have about you;
- to correct something that is wrong;
- to explain why we use it; or
- to stop using or delete it where the law allows.

You can speak to a member of Flourish staff or contact our Data Protection Lead using the details in section 2. We will listen and explain things in a way you can understand.