Manor Farm Fun Ltd

GDPR & Privacy Policy (Data Protection)

Manor Farm Fun
Manor Farm, Gossington, Slimbridge, Gloucester, Gloucestershire, GL2 7DN

Policy owner	CEO / Data Protection Lead - Hannah O'Brien
Approved	September 2026
Review	September 2027, or sooner following material legal/operational change
Applies to	Children and young people, parents/carers, staff, applicants, contractors, visitors, professionals and other indiv

Our commitment

Manor Farm Fun Ltd is committed to protecting personal information and respecting the privacy rights of children, families, staff and everyone with whom we work. This policy explains our approach to collecting, using, sharing, securing, retaining and disposing of personal information in accordance with the UK GDPR, the Data Protection Act 2018 and other applicable UK data-protection law.

Children merit particular protection. We will consider their best interests, developmental needs and expectations of privacy when designing services and information-handling arrangements.

1. Who is the data controller?

For processing where Manor Farm Fun Ltd determines why and how personal information is used, **Manor Farm Fun Ltd is the data controller**. Hannah O'Brien, CEO, is the organisation's senior data-protection lead and central contact for data-protection matters.

Contact: **hannah@manorfarmfun.co.uk**
Manor Farm, Gossington, Slimbridge, Gloucester, Gloucestershire, GL2 7DN
www.manorfarmfun.co.uk

Where we work with another organisation, the controller position depends on the particular activity. We may act as an independent controller, share information controller-to-controller, use a processor acting on our instructions, or act as a joint controller where both organisations jointly determine the purposes and essential means of processing.

2. Scope

This policy covers Manor Farm Fun's registered childcare, holiday-club, SEND/short-break and related services at its operating sites, together with bookings, family communications, staffing and administration. The organisation processes children's information including safeguarding, health, SEND and welfare information where necessary to provide safe and appropriate care.

This policy applies to information held electronically, on secure cloud systems, in email or communication systems, on authorised devices and in paper records.

3. Data-protection principles

- **Lawfulness, fairness and transparency:** use information lawfully and explain what we do with it.
- **Purpose limitation:** collect information for specified, explicit and legitimate purposes.

- **Data minimisation:** use only information that is adequate, relevant and necessary.
- **Accuracy:** take reasonable steps to keep information accurate and up to date.
- **Storage limitation:** retain identifiable information only for as long as necessary.
- **Integrity and confidentiality:** protect information using appropriate technical and organisational measures.
- **Accountability:** be able to demonstrate compliance through policies, records, training, contracts, risk assessment and audit.

4. Information we may process

- Names, dates of birth, addresses, contact details and family/contact relationships.
- Education, attendance, learning, assessment, SEND, EHCP and support information where relevant.
- Safeguarding, child-protection, welfare, behaviour, risk and incident information.
- Health, disability, allergy, medication, dietary and intimate-care information where needed.
- Photographs, video or audio where there is an identified and lawful purpose.
- Booking, payment, funding, invoicing and contractual information.
- Communications with families, schools, local authorities, health/social-care professionals and other agencies.
- Staff, volunteer and applicant information including recruitment, DBS/safeguarding, training, attendance, payroll and employment records.
- Website, booking-portal and system information such as account identifiers, IP/device information and audit logs where generated by our systems.

5. Special-category and criminal-offence information

Some of the information we need is particularly sensitive, including health, disability and other special-category information. We identify both an Article 6 lawful basis and an appropriate Article 9 condition before processing special-category information. Where criminal-offence information is processed, we ensure that the additional requirements of the Data Protection Act 2018 are met.

6. Why we use personal information and our lawful bases

The lawful basis depends on the purpose. We do not treat consent as the default basis for all processing.

Typical purpose	Potential Article 6 basis (as applicable)
Delivering booked/commissioned services and administering a contract, lega	Contract; legal obligation; legitimate interests; or public task where applicable to the specif
Safeguarding, child protection, welfare and risk management	Legal obligation; legitimate interests; vital interests; or public task, depending on the circur
Employment and workforce administration	Contract; legal obligation; legitimate interests
Financial, tax and regulatory records	Legal obligation; contract
Service improvement, security and administration	Legitimate interests, balanced against individuals' rights
Optional uses for which consent is genuinely appropriate	Consent - specific, informed, freely given and withdrawable

The exact lawful basis and, where relevant, special-category condition should be recorded in our Record of Processing Activities and supporting procedures. Safeguarding information may be shared without consent where there is a lawful basis and sharing is necessary and proportionate.

7. Children and young people's information

We recognise that children have data-protection rights in their own right. Privacy information directed to children will be concise, clear, accessible and appropriate to their age and understanding. Where helpful, we will use layered or

child-friendly explanations and explain risks and safeguards in an understandable way.

We will use strict access controls by default, avoid collecting excessive information and consider children's best interests when introducing new systems or significant changes to processing.

8. Sharing information

We may share relevant information with schools, local authorities, safeguarding partners, health and social-care professionals, emergency services, regulators, insurers, professional advisers, IT/system providers and other organisations where there is a lawful and necessary reason. We do not sell personal information.

Wickselm House Ltd CIC and Manor Farm Fun Ltd

The two organisations work closely together and some staff, children and families use or work across both services. Where necessary and lawful, relevant information may be shared between them to support continuity of provision, safeguarding, welfare, SEND support, risk management, staffing and administration.

The organisations may use agreed secure systems, including CPOMS and iPAL, on a shared or centrally administered basis. Access to a shared platform does not give a user authority to view all records. Access must be role-based and limited to a genuine need to know. Where the organisations jointly determine the purposes and essential means of a particular shared processing activity, they will document their respective responsibilities in a joint-controller/data-sharing arrangement.

9. Processors and suppliers

Where a supplier processes personal information only on our instructions, we will use an appropriate written data-processing contract and carry out proportionate due diligence. We will consider confidentiality, security, data location, subprocessors, retention, deletion/return arrangements, audit capability and assistance with data-subject rights and breaches.

10. International transfers

If personal information is transferred outside the UK, we will ensure that the transfer is lawful and protected by an applicable UK adequacy regulation or appropriate safeguards, together with any necessary transfer risk assessment and supplementary measures.

11. Security and access control

- Individual user accounts rather than shared credentials wherever systems permit.
- Role-based and need-to-know permissions, with heightened protection for safeguarding and sensitive records.
- Strong passwords and multi-factor authentication where available and appropriate.
- Prompt joiner/mover/leaver access changes.
- Secure storage, approved devices and encrypted or otherwise protected transmission where appropriate.
- Audit logs and proportionate monitoring of access.
- Staff confidentiality obligations, induction and refresher training.
- Secure disposal of paper and electronic information.

12. Data protection by design, DPIAs and new systems

Data protection will be considered at the start of new projects and throughout the information lifecycle. A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms and will be considered particularly carefully for children's information, large-scale sensitive information, monitoring, new technologies and material changes to shared-system arrangements.

13. Accuracy

We take reasonable steps to keep information accurate and relevant. Families, staff and other individuals should tell us when important contact, health, support or other information changes.

14. Retention and disposal

We retain information according to an approved retention schedule based on legal/regulatory requirements, safeguarding needs, contractual requirements, limitation periods and operational necessity. Different record types require different periods. We do not apply a single blanket retention period to all records.

When information is no longer required, it will be securely deleted, destroyed or anonymised. A record may need to be retained after a person stops using a service where there remains a lawful safeguarding, legal, regulatory or evidential reason.

15. Individual rights

- The right to be informed about how personal information is used.
- The right of access to personal information, subject to applicable exemptions and third-party rights.
- The right to rectification of inaccurate personal information.
- The right to erasure in circumstances where the law provides it.
- The right to restrict processing in applicable circumstances.
- The right to data portability where the statutory conditions apply.
- The right to object to certain processing, including direct marketing.
- Rights relating to solely automated decision-making where applicable.

Children may exercise their own rights where they have sufficient understanding. A parent/carer does not automatically own a child's data-protection rights. We will consider the child's competence, best interests, confidentiality and the circumstances of the request.

16. Subject access requests

Requests for personal information should be sent to **hannah@manorfarmfun.co.uk**. We may ask for proportionate evidence of identity or authority where necessary. We will search appropriate systems and records, consider third-party information and applicable exemptions, and respond within the statutory timeframe.

17. Personal-data breaches

Staff must report any suspected loss, misdirection, inappropriate access, disclosure, cyber incident or other personal-data breach immediately. We will contain and investigate the incident, record our assessment and notify the Information Commissioner's Office where the legal threshold is met. Where a breach is likely to result in a high risk to individuals, we will also communicate with affected individuals where required.

18. Photography, video and communications

Images, recordings and communications are personal information where an individual can be identified. We will identify a lawful purpose and basis, respect safeguarding and confidentiality, and use consent where consent is the appropriate basis for an optional use. Staff must use only approved communication channels and devices in accordance with our related policies.

19. Websites, portals and cookies

Our websites and online portals may process information needed to provide requested functions, administer accounts, maintain security and understand service use. Cookie and tracking technologies will be managed in accordance with applicable UK privacy and electronic-communications requirements. Where non-essential cookies require consent, users will be given an appropriate choice.

20. Staff responsibilities

- Access personal information only for authorised work purposes.
- Keep passwords, devices, records and conversations secure.
- Do not browse records out of curiosity or because technical access is available.
- Record information factually, proportionately and in the correct system.
- Follow safeguarding procedures and do not delay necessary safeguarding sharing.
- Report errors, breaches, excessive permissions and suspected security issues immediately.
- Complete required data-protection and information-security training.

21. Complaints

We encourage individuals to raise concerns with us first so that we can investigate and respond. Contact the CEO/Data Protection Lead at **hannah@manorfarmfun.co.uk**.

Individuals also have the right to complain to the Information Commissioner's Office (ICO), the UK's independent data-protection regulator. Current contact and complaint information is available from the ICO website.

22. Governance and review

We maintain proportionate accountability records including privacy notices, Records of Processing Activities, retention arrangements, processor contracts, data-sharing arrangements, DPIAs where required, training records and breach records. This policy will be reviewed at least annually and whenever there is a significant legal, regulatory, technological or service change.

Related documents

- Safeguarding and Child Protection Policy
- Record Keeping Policy
- E-Safety / Acceptable Use / Mobile Devices policies
- Access Control and Confidentiality procedures where applicable
- Data retention schedule
- Data breach procedure
- Subject access request procedure
- Wickselm House Ltd CIC / Manor Farm Fun Ltd Data Sharing & Shared Systems Arrangement
- Relevant staff and family privacy notices

Approval

Approved by	Hannah O'Brien, CEO / Data Protection Lead
Signature	_____
Date	_____
Next review	September 2027 or earlier if required

Policy note: This document is designed as an operational data-protection policy and privacy framework. The organisation should maintain more detailed schedules/procedures behind it (including the ROPA, retention schedule, lawful-basis record, DPIAs and processor register) rather than trying to place every operational detail in one public policy.