DATA SHARING & SHARED SYSTEMS PACK

Wickselm House Ltd CIC and Manor Farm Fun Ltd

Purpose: To document the controlled sharing of personal information between the two companies and the use of shared secure recording systems, including CPOMS and iPAL.

Organisations	Wickselm House Ltd CIC Manor Farm Fun Ltd
Senior responsible person	CEO / data protection lead: Hannah O'Brien
Scope	Children and families, staff, safeguarding, SEND, welfare, service delivery and administration
Version	Draft 1.0 - September 2026

1. Joint Data Controller & Information Sharing Arrangement

Parties

This arrangement is made between **Wickselm House Ltd CIC** ('Wickselm') and **Manor Farm Fun Ltd** ('MFF'). Each company is a separate legal entity and is a controller of personal data for the processing for which it determines the purposes and means.

Where the companies jointly determine the purposes and essential means of particular shared processing - including agreed use of a common record for children, families or staff who use or work across both organisations - they will treat themselves as **joint controllers for that shared processing** and allocate responsibilities through this arrangement.

Senior responsible person: The same CEO/data-protection lead oversees the arrangement for both companies. This does not remove the separate legal responsibilities of either company.

1.1 Purpose of sharing

- To provide safe, consistent and coordinated education, alternative provision, SEND short breaks, care-farm and related services.
- To maintain continuity where a child, family or member of staff engages with both organisations.
- To support safeguarding, child protection, welfare, SEND support, risk management and incident management.
- To avoid fragmented or contradictory records and unnecessary duplicate data entry.
- To enable proportionate operational administration, staffing, admissions, attendance, communication and service planning.
- To allow agreed secure systems such as CPOMS and iPAL to be administered centrally while maintaining appropriate access controls.

1.2 Principles

The parties will share only information that is necessary, relevant and proportionate for an identified purpose. A shared technical platform does **not** mean that every user is entitled to see every record. Access must follow role, site, case involvement and need-to-know.

Each organisation will comply with the UK GDPR, Data Protection Act 2018 and applicable safeguarding duties. Information will be processed fairly, transparently, accurately, securely and for no longer than necessary.

1.3 Categories of information that may be shared

- Child and family identification and contact information.
- Attendance, admissions, timetables, commissioned provision and service information.
- SEND information, EHCP-related information, reasonable adjustments and support needs where relevant.
- Safeguarding, child-protection and welfare information where sharing is necessary and lawful.
- Risk assessments, incidents, accidents, behaviour/support information and relevant medical or health information.
- Relevant communications with parents/carers, schools, local authorities and professionals.
- Staff identity, role, training, safeguarding, deployment and operational information where staff work across the organisations.
- System audit information showing access, changes and actions.

1.4 Lawful basis

The parties will identify and document the appropriate **Article 6 UK GDPR lawful basis** for each processing purpose. Where special-category data is processed, an appropriate **Article 9 condition** will also be identified and documented. Where criminal-offence data is processed, the parties will ensure the additional Data Protection Act 2018 requirements are met.

Consent will not be used merely as a blanket justification for routine safeguarding or service-delivery processing where another lawful basis is more appropriate. Where consent genuinely is the appropriate basis for a particular optional activity, it will be specific, informed, freely given and capable of withdrawal.

1.5 Shared systems: CPOMS and iPAL

- Users must have individual named accounts wherever the system permits; generic/shared logins should not be used for access to personal records.
- Permissions must be configured so staff see only the records and functions necessary for their role.
- Access to a shared platform is not authority to browse records unrelated to the user's work.
- Access must be removed or amended promptly when a role, site or employment changes.
- Audit logs should be retained and reviewed where inappropriate access is suspected.
- Multi-factor authentication and other security controls offered by the provider should be enabled where practicable.
- The organisations must maintain appropriate processor contracts/data-processing terms with each software supplier and establish where data is hosted and any international transfer arrangements.

1.6 Safeguarding

Nothing in this arrangement prevents or delays necessary safeguarding information sharing. Safeguarding information will be shared on a need-to-know basis, with the child's safety and applicable statutory guidance taking priority. Reasons for significant sharing decisions should be recorded.

1.7 Data subject rights and contact point

Individuals may exercise their data-protection rights against the relevant controller and, where processing is joint, against either joint controller. The organisations will cooperate so that requests are identified, routed and answered within the applicable statutory timescale.

The CEO/data-protection lead may act as the central contact point for queries and rights requests. Privacy notices should provide the current contact details.

1.8 Data breaches

Any suspected loss, unauthorised disclosure, inappropriate access or other personal-data breach affecting shared information must be reported immediately through the organisations' breach procedure. The parties will cooperate in containment, risk assessment, documentation, notification to the ICO where required, and communication to affected individuals where required.

1.9 Retention and deletion

Records will be retained according to an agreed retention schedule reflecting the nature of the record, safeguarding requirements, statutory obligations and limitation periods. Shared-system records must not be deleted merely because a person ceases to use one of the two services if there remains a lawful reason for the other organisation to retain them.

1.10 Review

This arrangement will be reviewed at least annually and sooner if there is a material change to the services, systems, ownership/controller relationship, categories of data, lawful bases, safeguarding arrangements or software providers.

1.11 Signatures

For Wickselm House Ltd CIC	For Manor Farm Fun Ltd
Name: Hannah O'Brien	Name: Hannah O'Brien
Capacity: CEO / authorised signatory	Capacity: CEO / authorised signatory
Signature: _____	Signature: _____
Date: _____	Date: _____

2. Parent & Family Privacy Notice - Shared Systems

Why you are receiving this information

Wickselm House Ltd CIC and Manor Farm Fun Ltd work closely together. Some children and families receive services from both organisations and some staff work across both. To provide safe, consistent support, the organisations use certain secure information-management systems on a shared basis, including CPOMS and iPAL.

This does not mean that all staff can see all information. Access is restricted according to a person's role, involvement with the child/family, safeguarding responsibilities and legitimate need to know.

What information may be shared?

- Contact and service information;
- attendance and provision records;
- SEND and support information;
- risk, welfare, incident and safeguarding information;
- relevant health information where needed to keep a child safe or provide appropriate support;
- relevant communications and professional information.

Why do we share it?

Information may be shared where necessary to deliver and coordinate services, keep children safe, meet safeguarding and legal responsibilities, manage risk, provide appropriate SEND support and maintain accurate records. We aim to avoid asking families to provide the same information repeatedly where it can lawfully and securely be used across the two organisations.

Do we rely on your consent?

We will always be transparent about how information is used. However, data-protection law does not require consent for every type of processing. For example, safeguarding information may need to be processed or shared without consent where there is an appropriate lawful basis. Where an activity genuinely requires consent, we will ask for it separately.

Who can access the information?

Only authorised personnel who require access for their work. Having an account on a shared system does not give a member of staff permission to view unrelated records. System access is subject to confidentiality, safeguarding and data-protection requirements and may be audited.

Your rights

You have rights under data-protection law, including rights relating to access, correction and, in some circumstances, restriction, objection or deletion. Some rights are subject to legal exemptions, particularly where safeguarding or third-party information is involved.

Questions or requests should be directed to the CEO/data-protection lead using the contact details published by Wickselm House Ltd CIC or Manor Farm Fun Ltd.

Privacy notice acknowledgement (optional administrative record)

I confirm that I have been provided with information explaining that Wickselm House Ltd CIC and Manor Farm Fun Ltd may lawfully share relevant information and use shared secure recording systems. I understand that this acknowledgement is not being used as blanket consent for processing that is carried out under another lawful basis.

Name	
Child's name (if applicable)	
Signature	
Date	

3. Staff Privacy & Confidentiality Notice - Shared Systems

Wickselm House Ltd CIC and Manor Farm Fun Ltd use certain secure recording and operational systems on a shared basis because staff, children and families may work with or receive services from both organisations. This may include CPOMS and iPAL.

Access is permission-based, not organisation-wide. Staff must access only information required for their role and current professional responsibilities.

Staff responsibilities

- Use only your own authorised account and keep credentials secure.
- Do not access a child's, family's or colleague's record out of curiosity or because the system technically allows access.
- Record information accurately, objectively, proportionately and in accordance with safeguarding and recording procedures.
- Do not copy information from one system, organisation or record into another unless there is a legitimate operational or safeguarding purpose.
- Do not download, photograph, email or otherwise export personal information unless authorised and secure.
- Report accidental access, misdirected information, lost devices, suspected compromise or other data incidents immediately.
- Respect role/site restrictions and tell management promptly if your access appears broader than required.
- Continue to follow safeguarding procedures: urgent child-protection concerns must not be delayed by uncertainty about data sharing.

Monitoring and audit

Access to shared systems may be logged and audited. Inappropriate access or disclosure may be treated as a confidentiality, safeguarding and/or disciplinary matter.

Staff personal information

Relevant staff information may also be processed across the two organisations where necessary for deployment, safeguarding, training, administration or other legitimate employment/operational purposes. Full staff privacy information should remain available separately.

Staff acknowledgement

I confirm that I have read and understood the shared-systems confidentiality requirements above and will access personal information only where necessary and authorised for my role.

Staff name	
Primary organisation / role	
Signature	
Date	

4. Implementation Checklist

Before putting the shared-system arrangement live, complete and retain evidence of the following:

- ■ Confirm and document which processing is separate-controller sharing and which, if any, is joint-controller processing.
- ■ Record the Article 6 lawful basis for each purpose and Article 9 condition for special-category data.
- ■ Complete or review a Data Protection Impact Assessment (DPIA), particularly for safeguarding/SEND data and shared access.
- ■ Update both organisations' full privacy notices and Records of Processing Activities (ROPA).
- ■ Check CPOMS/iPAL contracts and data-processing terms, hosting, subprocessors, retention and international transfers.
- ■ Create a permissions matrix showing which roles can see which sites/children/modules.
- ■ Use individual accounts and enable MFA where available.
- ■ Create joiner/mover/leaver procedures so access is changed promptly.
- ■ Document retention rules and responsibility for responding to subject access requests.
- ■ Train staff on need-to-know access, confidentiality, safeguarding sharing and breach reporting.
- ■ Review the arrangement annually and whenever the service model or software changes.