**Manor Farm Access Control and Confidentiality Policy**

**Policy Date:** 2 October 2025

**Review Date:** 2 October 2026

This policy sets out the procedures for managing access to Manor Farm’s information systems and data. It applies to all employees, contractors, and volunteers who are granted access to Manor Farm systems and ensures compliance with GDPR, safeguarding, and information security obligations.

# Starters

• Upon recruitment, new staff will only be granted access to systems relevant to their role, once pre-employment checks (including DBS clearance) are complete.
• Access rights are requested by the Hiring Manager and authorised by the Leadership Team.
• Login credentials are issued by the IT Manager and must not be shared.
• New staff will receive induction training covering data protection, confidentiality, safeguarding, and acceptable use of IT systems.

# Leavers

• When a staff member leaves Manor Farm, their system access will be revoked on or before their final working day.
• All accounts (including Microsoft 365, iPal, CPOMS, and other systems) will be deactivated by the IT Manager.
• Any Manor Farm devices, ID cards, or equipment must be returned before the final day of employment.
• Email accounts may be redirected or closed, in line with business needs and GDPR compliance.

# Movers

• Where a staff member changes role within Manor Farm, their system access will be reviewed and adjusted by the IT Manager in line with their new responsibilities.
• Old access rights will be removed if no longer necessary, and new permissions granted as appropriate.

• Managers must inform the IT Manager of any role change promptly to ensure access rights remain appropriate.

# Role-Based Access

• Access to systems and data is provided strictly on a need-to-know basis and aligned with each staff member’s role.
• Staff working in safeguarding, finance, or administration may have additional access rights, which must be approved by the Leadership Team.
• Periodic audits will be undertaken by the IT Manager to ensure access rights remain appropriate and proportionate.

# Confidentiality

• All staff are required to maintain confidentiality with respect to personal, sensitive, and safeguarding information.
• A confidentiality agreement is included in staff contracts, and breaches of confidentiality will be treated as a disciplinary matter.
• Information must not be disclosed to unauthorised persons or organisations.
• Staff must ensure that all IT equipment, including laptops and mobile devices, is password protected and encrypted.

# Remote Access

• Remote access to Manor Farm systems is only permitted through secure, approved solutions.
• Staff must not use personal email or cloud services to store or share Manor Farm data.
• When remote access is no longer required (e.g., upon leaving employment), all rights will be revoked immediately by the IT Manager.

# Monitoring and Review

• The IT Manager will conduct regular reviews of access rights and audit trails to ensure compliance.
• This policy will be reviewed annually, or sooner if required by changes in legislation, technology, or organisational needs.