June 2026

Data Protection Policy



M&C PROPERTY



Company:
Madigan Cunningham Ltd t/a M&C Property

Registered address:
9 Lower Cecil Street, Limerick

Website: www.mcp.ie

Policy owner: Associate Director

Applies to:
All employees, contractors and temporary workers across Athlone, Dublin, Galway and Limerick offices, including remote workers

Last reviewed: June 2026

1. Purpose

This policy explains how Madigan Cunningham Ltd t/a M&C Property manages personal data in accordance with the General Data Protection Regulation, the Data Protection Act 2018 and guidance issued by the Irish Data Protection Commission. It is intended to help staff handle personal data lawfully, fairly, transparently and securely in the delivery of student accommodation, sales, lettings and property management services.

2. Scope

This policy applies to all personal data processed by the company in paper or electronic form. It covers data processed in the company's own capacity as controller, including employee and business administration data, and data processed on behalf of clients where clients are the data controllers and M&C Property acts as processor.

3. Business Activities Covered

- **Student accommodation management and administration.**
- **Residential and commercial sales.**
- **Residential and commercial lettings.**
- **Property management for multi-unit and commercial developments.**
- **Client, supplier, contractor and internal business administration.**

4. Roles and Responsibilities

The Associate Director is the policy owner and is responsible for oversight of this policy, periodic review, staff awareness and escalation of data protection matters. The company has not appointed a Data Protection Officer. All staff are responsible for handling personal data securely, only using it for authorised business purposes, and reporting any suspected data breach or data protection concern promptly.

5. Controller and Processor Position

M&C Property may act as a data controller for its own business data, including employee records, payroll administration, supplier records, internal IT administration and general company operations. In many property management and agency activities, M&C Property processes personal data on behalf of clients who are the data controllers. Where acting as processor, the company will process personal data only on documented client instructions, maintain appropriate security measures, assist clients with data protection obligations where required, and ensure that any approved sub-processors are subject to appropriate contractual safeguards.

6. Personal Data We Process

- **Employees:** identification, contact, payroll, employment, performance, training, leave and emergency contact details.
- **Students, parents, tenants, landlords, applicants, buyers and sellers:** contact details, application information & identification, tenancy or transaction details, correspondence and supporting documentation required for the relevant service.
- **Contractors and suppliers:** contact details, service records, access arrangements and payment administration information.
- **Emergency contacts:** names, contact details and relationship information where required for accommodation, tenancy or employment purposes.
- **Operational property details:** key, fob and parking allocation details where these identify or relate to an individual.

Applicant information is retained only while an application is being considered. If an application is unsuccessful, the information is deleted unless there is a lawful reason to retain it for a limited period. If the application is successful, the relevant information is transferred to the appropriate tenancy, student accommodation, sales, lettings, property management or employment record.

7. Lawful Bases for Processing

Personal data must only be processed where there is a lawful basis. Depending on the activity, the company may rely on contract, legal obligation, legitimate interests, consent, vital interests or client instructions where the company acts as processor. Staff must ensure that personal data is collected only where necessary, used only for the relevant purpose, kept accurate and shared only where authorised.

8. Systems and Locations of Data

The company uses Microsoft 365, Outlook, Teams, SharePoint, OneDrive, Sage, Glantus, TCAS, Fixflo, KPR, Blockman and Letman for business and operational data. The company may also use Adobe, Dropbox, Google services, Copilot and ChatGPT. Personal data must be stored only in approved company systems and must not be transferred to personal email accounts, personal cloud storage or unapproved devices.

9. Use of AI and Cloud Tools

Staff must take care when using AI or cloud-based tools such as Copilot, ChatGPT, Adobe, Dropbox or Google services. Personal data, confidential client information, commercially sensitive information, identification documents, tenancy records, employee records or financial information must not be entered into public or unapproved AI tools. Approved AI or cloud tools may only be used in accordance with company instructions, contractual terms, confidentiality obligations and applicable data protection requirements.

10. Security Measures

- **Multi-factor authentication for company systems where available.**
- **Password manager use and strong password practices.**
- **Company laptops and mobile phones for remote working.**
- **Backups to protect availability and resilience of company data.**
- **Encryption where appropriate for devices, files or transmissions.**
- **Secure shredding for confidential paper records.**
- **Access controls so staff only access data needed for their role.**
- **Care when sending emails, attachments and shared links.**

11. Remote Working

Staff working remotely must use company-issued laptops and mobile phones, keep devices secure, prevent unauthorised viewing of personal data, use approved systems only, and report lost or stolen devices immediately. Paper records should not be removed from offices unless necessary and authorised, and must be transported and stored securely.

12. Third-Party Processors and Professional Advisers

The company may share personal data with payroll providers, accountants, solicitors and cloud software providers where necessary for company administration and legal, accounting, payroll or operational purposes. Where a third party processes personal data on behalf of the company, appropriate processor terms should be in place. Where data is processed on behalf of clients, any sharing with third parties must be consistent with client instructions, contractual arrangements and applicable law.

13. Data Subject Rights

Individuals may have rights to access, rectify, erase, restrict, object to or transfer their personal data, and may have rights relating to consent or automated decision-making where relevant. Requests should be referred promptly to the Associate Director. Where the company acts as processor for a client, requests must be referred to the relevant client controller unless the company has been authorised to respond.

14. Personal Data Breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending personal data to the wrong recipient, losing a device or file, unauthorised access to a system, ransomware, accidental deletion or disclosure of paper records. Staff must report suspected breaches immediately to the Associate Director. The company will assess the breach, contain it, document it, notify the relevant client controller where applicable, and determine whether notification to the Data Protection Commission or affected individuals is required.

15. CCTV

The company does not operate CCTV. If CCTV is introduced in the future, a separate CCTV policy, signage, lawful basis assessment and retention period will be required before use.

16. Retention and Deletion

Personal data must not be kept for longer than necessary. Retention periods should reflect legal obligations, contract requirements, client instructions, limitation periods, operational needs and the principle of data minimisation. Records should be securely deleted, anonymised, archived or shredded at the end of the relevant retention period.

Record type	Retention period	Legal / operational basis and notes
Unsuccessful tenancy, student accommodation, sales or lettings applications	Delete within 14 days of the application outcome unless a complaint, dispute or legal reason requires longer retention	Retain only what is needed to deal with follow-up queries, complaints or equality/non-discrimination issues. Earlier deletion should apply where there is no continuing need.
Successful applications	Transfer to the relevant active tenancy, accommodation, sales, lettings, property management or employment file	Application-stage documents should be reviewed and unnecessary duplicates deleted once the active file is opened.
Residential and commercial tenancy / lettings files	Duration of tenancy or instruction plus 6 years after closure	Reflects contract, limitation, tax/accounting and dispute-management requirements. Where M&C Property acts as processor, client controller instructions take precedence unless unlawful.
Residential and commercial sales files	Duration of instruction or transaction plus 6 years after closure	Retain core transaction, correspondence and financial records required for audit, legal and dispute purposes.
Student accommodation files	Duration of accommodation relationship plus 6 years after closure	Retain records needed for contract, payment, property management, complaints, incident and dispute purposes. Delete emergency contact and access details sooner where no longer required.
Property management records for multi-unit and commercial developments	Duration of management appointment plus 6 years after the end of the appointment, unless client instructions require a different lawful period	Retain records needed for service charge administration, contractor management, insurance, health and safety, disputes, accounting and client handover.
Accounting, invoices, supplier payments and tax records	Minimum 6 years after the end of the relevant financial year	Irish company and tax record-keeping requirements generally require financial and tax records to be retained for at least 6 years. Confirm any extended period with the accountant.

Record type	Retention period	Legal / operational basis and notes
Payroll records, payslips and payroll tax documentation	Minimum 6 years	Retain for Revenue, payroll audit and employment compliance purposes.
Employee personnel file	Duration of employment plus 6 years after employment ends	Retain contract, role, salary, disciplinary, grievance, performance, training and termination records for employment, limitation and dispute purposes. Review older material and delete unnecessary duplicates.
Working time, annual leave, public holiday and rest break records	3 years	Employers must retain working time records for 3 years. Payroll or related records may need to be retained for longer where they form part of payroll or tax records.
Parental leave, force majeure leave and carers leave records	8 years where applicable	Retain statutory leave records for the relevant employment law retention period.
Recruitment records for unsuccessful employee candidates	6 to 12 months after the recruitment decision unless a complaint, dispute or legal reason requires longer retention	Use the shorter period where possible. Retain only where needed for recruitment audit, equality, complaint or legal defence purposes.
Contractor and supplier due diligence and service records	Duration of relationship plus 6 years	Retain contracts, insurance, health and safety, payment and service records needed for audit, legal and dispute purposes.
Emergency contact details	While the relevant relationship is active; delete promptly when no longer required	Review when an employee, tenant, student or other relationship ends, or when updated information is provided.
Key, fob, access and parking allocation records	While access or allocation is active; delete or archive within 3 months after return, cancellation or reallocation unless needed for a dispute or investigation	Keep only current and auditable access records. Remove obsolete allocations promptly.
Data subject rights request records	6 years after closure of the request	Retain request, identity verification, decision, response and any exemption analysis for accountability and dispute purposes.
Personal data breach records and breach register	6 years after closure of the incident, or longer if litigation, regulator engagement or client instruction requires	Controllers must document personal data breaches, decisions, risk assessment, notifications and remedial actions. Processor incidents should also be recorded and reported to the client controller.

Record type	Retention period	Legal / operational basis and notes
Training records for data protection, cyber security and breach reporting	6 years	Retain evidence of staff awareness and compliance activity.
System access logs and audit logs	Normally 6 to 12 months, unless required longer for security investigation, legal hold, client instruction or system configuration	Retention should balance security monitoring needs with data minimisation.
Backups	In line with the company backup cycle; restore copies should not be used as long-term archives	Deleted records may remain in backups until the ordinary backup cycle overwrites them. Access to backups should be restricted.
Paper records marked for confidential disposal	Dispose of as soon as no longer required	Use secure shredding or approved confidential waste disposal and keep disposal evidence where available.

17. Training and Awareness

Staff should receive appropriate data protection awareness and practical guidance on secure handling of personal data, email use, remote working, breach reporting, phishing risks, cloud tools and AI tool restrictions. Refresher training should be provided periodically and when systems, services or legal requirements change. The training should be practical, role-based and focused on the types of personal data handled by M&C Property in student accommodation, sales, lettings and property management.

18. Review

This policy should be reviewed at least annually, or sooner if there are significant changes to services, systems, suppliers, office arrangements, legal requirements, client instructions or data protection risks.

Thank you!

LIMERICK
9 Lower Cecil St,
Limerick
V94 K2Y2
T: 061 432 777

GALWAY
Unit 5A
Liosban Business Park
Tuam Road,
Galway, H91 V294
T: 091 397 497

ATHLONE
Unit 3 Summerhill
Business Park Crannagh
More, Summerhill,
Athlone, Co. Westmeath,
N37 T2R7
T: 090 649 0111

DUBLIN
176 Lower Rathmines Road,
Rathmines,
Dublin 6,
D06 TY47
T: 01 482 5842

M&C PROPERTY

OConnor Shannon
Now part of
M&C Property

Madigan Cunningham Ltd. trading as M&C Property. Reg. Address: 9 Lower Cecil Street, Limerick.
Company Reg. No. 441682 VAT No. IE 9660020R PSRA Licence No. 001231