Murrays Bar & Grill

33 – 34 O'Connell Street Upper

Rotunda

Dublin 1.

CCTV Data Protection Policy

Organisation Name: O'Connell Street Inns LTD T/A Murrays Bar & Grill

Data Controller: Murrays Bar & Grill, 33-34 O'Connell Street Upper, Rotunda, D1

Data Protection Officer (DPO) / Contact: Neil Byrne

Effective Date: October 2026

Review Date: October 2027

Sector: Hospitality

Data Protection Officer: Neil Byrne (neil@murraypubgroup.com)

CCTV footage is stored for 30 days at which time it is overwritten.

1. Purpose and Lawfulness

Murrays Bar & Grill operates a Closed-Circuit Television (CCTV) system for the following legitimate purposes:

• Protecting premises, buildings, and physical assets.

• Promoting the health and safety of staff, visitors, and the public.

• Deterring and detecting crime, theft, vandalism, or anti-social behaviour.

• Supporting An Garda Síochána or relevant authorities in investigating incidents.

Processing is carried out under Article 6(1)(f) GDPR (legitimate interests). Where required by risk or scale, a Data Protection Impact Assessment (DPIA) is completed prior to installation or significant system changes.

2. Scope and Camera Locations

This policy applies to all overt CCTV cameras operated at [Insert Address/Sites].

• Monitored Areas: Main entrances/exits, bars & lounges, external perimeters, cash/storage areas, public restrooms common areas (restroom cubicles and urinals are not covered by CCTV)

• Restricted / Non-Monitored Areas: Cameras do not cover areas where individuals have a high expectation of privacy, such as toilet cubicles or urinals, changing facilities, or private rest areas.

• Prohibited Uses: CCTV is not used for routine employee performance evaluation, monitoring political or religious activity, or covert surveillance unless strictly justified and documented under law.

• Neighbouring / Public Areas: Cameras are positioned to minimize capture of public footpaths, roads, or neighbouring properties.

3. Signage and Transparency

Clear, prominent signage is displayed at entrances and near camera locations. Signs state:

• That CCTV recording is in operation.

• The purpose of the recording.

• The identity and contact details of the Data Controller / DPO. In this case Neil Byrne, General Manager, contact neil@murraypubgroup.com

4. Storage, Security, and Retention

• Security: Footage is stored securely on [encrypted servers / locked recording equipment] in a restricted area, protected by strong access controls and passwords. Access logs are maintained.

• Retention Period: Unless required for an active investigation, legal claim, prosecution, or statutory request, footage is automatically overwritten after 30 calendar days.

5. Access and Disclosure to Third Parties

• Internal Access: Access to live or recorded footage is strictly limited to authorised personnel [e.g., Senior Managers, DPO].

• An Garda Síochána and Legal Authorities: Disclosures are made only where lawful, typically following a written request specifying the incident details and timeframe, or under court order/legal obligation.

• Third-Party Processors: Any external installer or monitoring contractor acting as a data processor must be bound by a written data processing agreement and security obligations.

6. Data Subject Rights and Requests

Individuals whose images are captured have rights under GDPR, including the right to request access to their personal data (Subject Access Request), erasure, restriction, or objection, subject to legal exemptions.

• Requests must include sufficient details (such as date, approximate time, location, and identifying description) to locate the footage.

• Where releasing footage would reveal third parties' personal data, faces/identifiers of other individuals will be redacted or blurred before disclosure.

• Individuals also have the right to lodge a complaint with the Data Protection Commission (DPC) in Ireland.

7. Policy Review and Breaches

Any suspected security breach or unauthorised disclosure of CCTV footage must be reported immediately to the DPO and assessed under GDPR breach notification rules. This policy is reviewed annually or when operational or legal changes require.