Appendix 12
DUNCAN'S Minibus Policy
Safe Use of Minibuses
Date: 14 May 2025

Duncan Private Hire

Confidentiality & Code of Conduct Policy

Effective Date: 14 May 2025
Applies To: All Staff and Contractors

1. Purpose

This policy outlines Duncan Private Hire's commitment to maintaining the highest standards of confidentiality when handling client or patient-identifiable information. It ensures compliance with legal obligations including the Data Protection Act 1998, Human Rights Act 1998, and related standards within healthcare and public services.

2. Policy Overview

As a service provider working closely with NHS organisations, Duncan Private Hire recognises the importance of handling sensitive data with care, discretion, and integrity. Staff may come into contact with personal, health, or identifying information during the course of their duties. Such data must be treated with strict confidentiality, used appropriately, and shared only when legally justified and authorised.

All employees are personally accountable for protecting the confidentiality of client/patient-identifiable information.

3. Scope

This policy applies to:

- All client/patient-identifiable information in any format (paper, digital, verbal).
- All staff, contractors, temporary workers, and anyone operating on behalf of Duncan Private Hire.

4. Legal Framework

4.1 Data Protection Act 1998 (DPA)
Controls the use, storage, and processing of personal data, protecting individuals' privacy.

4.2 Common Law Duty of Confidentiality
Confidential information must not be shared without consent, unless explicitly authorised by law.

4.3 Human Rights Act 1998
Recognises the individual's right to privacy and family life.

4.4 Administrative Law
Public bodies must operate within legal powers when managing personal information, especially around consent.

5. Definitions

Patient/Client-Identifiable Information (PII):
Any data that can directly or indirectly identify an individual, including:

- Names, initials, addresses, dates of birth, NHS numbers
- Postcodes, occupations, ethnic background, and combinations of data points

Unauthorised Persons:
Anyone who does not have a legitimate, role-based reason to access specific confidential information.

6. Key Principles of Data Confidentiality

All staff must follow these principles when handling confidential information:

1. Justify the purpose for using confidential data.
2. Limit access strictly to those who need to know.
3. Use the minimum necessary information.
4. Obtain informed consent where required.
5. Ensure physical and digital security of records.
6. Follow data retention and destruction protocols.
7. Be aware of and comply with legal responsibilities.

7. Practical Guidelines

7.1 Handling and Access

- Do not access information unless required for your role.
- Never view your own or others' records unless formally authorised.
- When in doubt, ask your manager before accessing or sharing information.

7.2 Physical Security

- Keep paper records secure and out of public view.
- Lock rooms or secure cabinets where confidential records are stored.
- Adopt a clear desk policy – no sensitive information should be left unattended.

7.3 Electronic Data Security

- Always log off or lock screens when away from your workstation.
- Use strong, private passwords. Never share login credentials.
- Ensure all digital files containing personal information are encrypted and stored securely.
- Do not store PII on portable devices unless absolutely necessary and authorised.

7.4 Data Transfer

- Mark all documents containing personal data as "CONFIDENTIAL".
- Use sealed and clearly addressed envelopes for internal and external mail.
- Confirm recipient details before sending information.
- Avoid including unnecessary identifiers; redact where appropriate.
- For digital transfers, use secure, encrypted systems or authorised platforms.

7.5 Conversations & Verbal Communication

- Avoid discussing personal information in public or non-secure areas (e.g. hallways, waiting rooms).
- When discussing sensitive matters by phone, confirm the recipient's identity.
- Keep meetings private, and limit the sharing of identifiable details.

8. Off-Site and Portable Equipment Use

If using mobile devices or transporting confidential information:

- Secure physical devices and records at all times.
- Obtain permission before removing information from site.
- Ensure encryption and password protection on all devices.
- Never leave devices in vehicles unattended.

9. Breaches of Confidentiality

Breaches of this policy are serious offences and may result in:

- Disciplinary action, including termination of employment.
- Legal consequences for both individuals and Duncan Private Hire.
- Reputational damage to our organisation and NHS partners.

If you suspect a breach or receive data in error, **report it immediately** to your line manager.

10. Staff Responsibilities

All staff must:

- Understand their role in maintaining confidentiality.
- Participate in regular training on data protection.
- Know how to report concerns and breaches.
- Respect client/patient privacy as they would expect for themselves.

11. Final Note

Client/patient trust is built on our commitment to protecting their privacy. By following this policy, we uphold the integrity and professionalism of Duncan Private Hire and our service to the community.

For any questions or clarifications, please contact your line manager.

Approved by:
Duncan Private Hire Management Team
Effective Date: 14 May 2025
Review Date: 14 May 2026