



Data Protection Policy

**Clear governance.
Strong practice.
Safe services.**



**Clear governance.
Strong practice.
Safe services.**

1. Purpose and Scope

D2 PropCo delivers accommodation and property related services to people experiencing homelessness, housing instability or significant vulnerability. In doing so, the organisation routinely handles highly sensitive personal information, including medical details, risk information, offending history, safeguarding concerns, financial circumstances and tenancy related data. This information is essential to delivering safe, lawful and effective services, but it also carries significant risk if mishandled.

A strong approach to data protection ensures that personal information is collected, used, stored and shared in a way that protects individuals, supports safe decision making and maintains trust with residents, staff, partners and regulators. Data protection is not only a legal requirement; it is a core part of safeguarding, risk management, professional conduct and organisational integrity.

This policy sets out D2's strategic approach to information governance and applies to all staff, managers, directors, contractors, volunteers and partners who access or process personal data on behalf of the organisation.

2. Legal and Regulatory Framework

D2's data responsibilities are shaped by a clear legal framework that governs how personal information must be handled. Compliance with these requirements ensures that decisions are lawful, defensible and aligned with best practice. It also protects the rights of individuals whose information we hold and supports the organisation's credibility with commissioners, regulators and partners. D2's data protection approach aligns with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- Freedom of Information Act 2000 (where applicable)
- Information Commissioner's Office (IC) guidance and Codes of Practice
- Common law duty of confidentiality
- Welsh Government and local authority data sharing expectations
- Safer recruitment and DBS requirements
- Surveillance Camera Code of Practice (for CCTV use)

This framework underpins safe practice, protects vulnerable people and ensures D2 meets its obligations as a responsible data controller.



**Clear governance.
Strong practice.
Safe services.**

3. Definitions

Clear definitions support consistent understanding across the organisation and ensure that staff, managers and contractors interpret key terms in the same way. Because D2 handles complex, sensitive and high risk information, clarity of language is essential to safe practice, lawful decision making and effective governance.

These definitions provide a shared foundation for how data is understood, managed and protected across all services.

Personal Data – Information relating to an identified or identifiable individual.

Special Category Data – Sensitive information requiring enhanced protection, including health data, racial or ethnic origin, religious beliefs, sexual orientation and biometric data.

Criminal Offence Information – GDPR gives extra protection to personal data relating to criminal convictions and offences or related security measures.

Data Controller – The organisation that determines why and how personal data is processed. D2 PropCo is the data controller for all information processed in connection with its services.

Data Processor – Any individual or organisation that processes personal data on behalf of the data controller. Contractors may act as data processors for D2.

Processing – Any action performed on personal data, including collecting, storing, viewing, sharing, recording, deleting, analysing or transmitting information.

Data Breach – Any incident that results in the loss, unauthorised access, disclosure, alteration or destruction of personal data.

CCTV Data – Images or recordings captured by D2's surveillance systems.

Data Protection Officer (DPO) – The individual responsible for overseeing data protection compliance and acting as the point of contact with the IC.



**Clear governance.
Strong practice.
Safe services.**

4. Data Subject Rights

D2 will establish processes to ensure individuals can exercise their rights under UK GDPR and the Data Protection Act 2018. Requests will be managed consistently, recorded appropriately and responded to within statutory timescale.

5. Data Protection Principles

D2's workforce handles information that is often sensitive, complex and central to people's safety and wellbeing. Staff across all roles, from frontline teams to office based colleagues, rely on accurate, lawful and secure information to make decisions that can directly affect the lives of vulnerable individuals.

Clear data protection principles ensure that personal information is treated with consistency, respect and professionalism, regardless of who is handling it or where it is stored.

These principles provide the foundation for safe practice, guide staff when navigating difficult or ambiguous situations, and help the organisation demonstrate accountability as a responsible data controller. They apply to everyone and shape how D2 protects the rights, dignity and privacy of the people it supports. D2's principles:

- **Lawfulness, fairness and transparency** – personal data is processed legally and openly.
- **Purpose limitation** – information is collected for clear, legitimate reasons and not used inappropriately.
- **Data minimisation** – only the information necessary for safe and effective service delivery is collected.
- **Accuracy** – information is kept up to date and corrected promptly when inaccurate.
- **Storage limitation** – data is retained only for as long as necessary and disposed of securely.
- **Integrity and confidentiality** – information is protected from loss, misuse, unauthorised access or disclosure.
- **Accountability** – D2 demonstrates compliance through clear governance, training and assurance.

D2 will maintain records describing its processing activities, systems, data flows and information assets to support accountability and risk management.

D2 will maintain a Data Retention Schedule defining retention periods and secure disposal requirements for personal information.



**Our Purpose is Shelter.
Our Values are Strength.
Our Promise is Dignity.**

D2 will maintain appropriate privacy notices for residents, staff, job applicants, contractors and other individuals whose information is processed.

D2 will ensure appropriate contractual arrangements, including Data Processing Agreements, are in place where third parties process personal data on its behalf.

All staff, managers and contractors will receive data protection awareness training appropriate to their role.

6. Data Protection Risks and Consequences

Poor data protection practice exposes D2 to significant organisational risk. Because the organisation handles highly sensitive information relating to vulnerable people, any breach (accidental or deliberate) can cause real harm, undermine trust and damage D2's credibility with residents, partners and commissioners.

Data breaches may result in regulatory action by the Information Commissioner's Office (IC), including enforcement notices, mandatory audits or financial penalties. In addition, individuals affected by a breach may pursue legal claims for distress or harm, and commissioners may question D2's suitability to deliver contracted services.

Protecting personal data is therefore essential not only for safety and dignity, but for safeguarding D2's reputation, financial stability and long term viability as a service provider.

Data Protection Impact Assessments (DPIAs) will be undertaken where new systems, services, technologies or processing activities may present elevated privacy risks.

7. Sensitive and High-Risk Information

D2 holds information that goes far beyond routine personal data. The organisation manages details about people's health, risks, behaviours, vulnerabilities, offending history and lived experience, information that, if mishandled, could cause real harm, undermine trust or compromise safety.

Because this data is central to safeguarding, risk management and service delivery, it must be handled with heightened care, strict controls and a clear understanding of the potential impact on individuals. Protecting sensitive information is not only a legal requirement; it is a core part of D2's duty of care to residents, staff and partners.



**Clear governance.
Strong practice.
Safe services.**

D2 will:

- apply enhanced controls to all sensitive and high risk data
- ensure only authorised staff access this information
- maintain accurate, up to date records
- ensure secure storage and transmission
- restrict sharing to lawful, necessary and proportionate circumstances

Contractor Risk

D2 works with contractors who may access sensitive information. As the data controller, D2 remains legally responsible for how this information is handled. Contractors must therefore meet D2's standards in full and report any concerns or breaches immediately.

8. CCTV and Surveillance Data

All D2 properties are equipped with CCTV systems that operate continuously. CCTV is used to support resident safety, protect staff, deter crime, manage incidents and maintain secure environments. Because CCTV captures identifiable images and behavioural information, it is classified as personal data and must be managed with the same rigour as all other sensitive information.

D2 will:

- ensure CCTV use is lawful, proportionate and clearly communicated
- display appropriate signage
- restrict access to authorised staff
- review footage daily for safety and incident management
- retain footage only for approved periods
- store footage securely and encrypted
- comply with the Surveillance Camera Code of Practice
- record and justify any sharing of footage



**Clear governance.
Strong practice.
Safe services.**

9. Information Security and Access Control

Strong information security is essential to protecting the people D2 supports and maintaining the integrity of the organisation. Staff across all roles, from frontline teams to office based colleagues, rely on accurate, secure and accessible information to make safe decisions. At the same time, the organisation must guard against unauthorised access, data loss, cyber threats and human error. Effective security is not just about technology; it is about culture, behaviour and shared responsibility.

D2 will:

- maintain secure digital systems with appropriate access controls
- ensure staff only access information necessary for their role
- use strong passwords, MFA and secure devices
- encrypt data where appropriate
- ensure paper records are stored securely
- report breaches immediately
- ensure contractors meet equivalent security standards

D2 will maintain supporting information security controls and policies.

10. Data Sharing and Partnership Working

D2 works within a complex network of partners, including local authorities, health services, police, support agencies and contractors. Sharing information is often essential to protect residents, manage risk and deliver coordinated services, but it must always be lawful, proportionate and justifiable. Poorly judged information sharing can expose individuals to harm, while failing to share when necessary can undermine safety and decision making.

D2 will:

- share information only where there is a clear legal basis
- ensure staff understand thresholds for consent, vital interests and safeguarding
- maintain data sharing agreements with key partners
- record decisions to share information
- ensure contractors comply with D2's standards



**Clear governance.
Strong practice.
Safe services.**

11. Governance, Roles and Responsibilities

Effective data protection depends on clear governance and shared accountability across the organisation. Every member of staff, regardless of role, seniority or location, has a part to play in protecting personal information and ensuring lawful practice. At the same time, the Board, CEO, Senior Management Team and Data Protection Officer each hold distinct responsibilities that shape how data is managed, monitored and assured.

Board

- Sets strategic expectations
- Receives assurance on compliance, breaches and risks

CEO

- Accountable for lawful and effective data management
- Ensures systems, resources and policies are in place

Senior Management Team

- Leads implementation
- Monitors risks, breaches and compliance
- Reports assurance to the Board

Data Protection Officer

The Organisation has chosen to appoint a Data Protection Lead to manage day-to-day data protection operations, rather than a formal, statutory Data Protection Officer (DPO).

Data Protection Lead

- Governance & Board Assurance
- Data Mapping & Accountability (ROPA)
- DPIAs & Privacy Risk Management
- Breaches, Complaints & DSAR Oversight
- Training, Awareness & Data Champions
- Supplier, Processor & Data Sharing Assurance



**Clear governance.
Strong practice.
Safe services.**

Managers

- Ensure staff follow requirements
- Escalate concerns promptly
- Support staff understanding

All Staff

- Handle information lawfully and securely
- Report breaches immediately
- Access only what is necessary

Contractors and Partners

- Must comply with D2's standards
- Must report incidents immediately
- Must ensure their staff are trained and competent

12. Monitoring, Assurance and Continuous Improvement

Data protection is not a static requirement; it is an ongoing process that evolves as risks, technology and organisational needs change. Regular monitoring and assurance help D2 understand how information is being handled across services, identify emerging issues and take action before harm occurs. Trends in breaches, access patterns, training compliance and CCTV usage provide valuable insight into the organisation's data health.

D2 will monitor:

- data breaches and near misses
- access logs and system activity
- CCTV usage and retention
- training compliance
- data sharing decisions
- audit findings
- staff feedback

Findings will inform an annual Information Governance and Data Protection Report to the Board.



**Clear governance.
Strong practice.
Safe services.**

13. Review

This policy will be reviewed annually, or sooner if legislation, regulation or organisational needs change.

14. Policy Approval and Version Control

Policy Owner:	Managing Director
Approval:	Board
Date:	09/04/2026
Tier:	1 – Core Governance Policy
Review Cycle:	Annual

Lets Talk

CARDIFF: 02920 024429 / **CAERPHILLY:** 07816 897244

EMAIL: info@d2propco.com

CARDIFF (SOUTH)

Millgrove House,
Parc Ty Glas,
Llanishen, Cardiff
CF14 5DU

FLINTSHIRE (NORTH)

11 Chester Road
West Shotton
Deeside
CH5 1B

WAREHOUSE

Unit 22, Dyffryn Court
Dyffryn Ind.Est.
Caerphilly
CF82 7TT