PRIVACY POLICY

Data Protection, Information Governance and Data Sharing

Approved by	Shernette Pringle, Registered Manager
Effective date	01 July 2026
Last reviewed	01 July 2026
Next review due	01 July 2027, or sooner following any change in law, DPS contract terms, or ICO guidance
Applies to	All service users, their families/representatives, staff, workers, contractors, and volunteers of Pringle's Care Services Limited
Related documents	Privacy Promise; Safeguarding Adults and Whistleblowing Policy; Business Continuity Plan; Data Security and Protection Toolkit (DSPT) submission; Ealing Council Community Services DPS Agreement (incl. Schedule 7 Information Sharing Protocol and Clause 24 Data Protection)

1. Who We Are

Pringle's Care Services Limited (“Pringle's”, “we”, “us”, “our”) is a company registered in England and Wales under company number 06902046. Our registered office is at Crown House, North Circular Road, Park Royal, London, NW10 7PN. Our branch office used for service delivery is registered at 405–406 Crown House, North Circular Road, London, NW10 7PN, and is registered with the Care Quality Commission (CQC) under registration number 1-134218947.

We provide domiciliary care, extra care, day and evening opportunities, and floating support services, including services commissioned by the London Borough of Ealing under its Community Services Dynamic Purchasing System (DPS) for Adults' and Children's Domiciliary Care, Extra Care, Adult Day and Evening Opportunities, and Adult Floating Support Services (“the DPS Agreement”).

This policy applies to personal data we handle in our own right as a care provider and personal data we handle under our contractual obligations to the London Borough of Ealing (“the Council”/“the Authority”) and any other local authority that commissions our services through a similar arrangement.

2. Purpose and Scope of This Policy

This Privacy Policy sits alongside our shorter Privacy Promise and provides the fuller level of detail required by the DPS Agreement, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and CQC information governance requirements. Where our Privacy Promise gives a summary, this Policy gives the full explanation, including the legal bases we rely on, exactly what data we collect and why, who we share it with, how long we keep it, and how we keep it secure.

This Policy covers personal data relating to:

- Service users and, where relevant, their families, carers, and representatives;
- Staff, workers, contractors, and volunteers (see Section 12); and
- Any other individual whose personal data we process in connection with delivering our services, including referrers, health and social care professionals, and next of kin/emergency contacts.

3. Legal Framework We Comply With

We process personal data in accordance with:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended);
- The Human Rights Act 1998 (Article 8 – right to respect for private and family life);
- The Common Law Duty of Confidentiality;

- The Caldicott Principles for handling service user identifiable information;
- The Mental Capacity Act 2005, in relation to service users who may lack capacity to consent to information sharing;
- The Care Act 2014; and
- The Freedom of Information Act 2000, insofar as we are required to assist the Council in meeting its own obligations under that Act.

These are the same laws referenced in Schedule 7 (Information Sharing Protocol) of the DPS Agreement, which governs how information is shared between Pringle's, the Council, and other partner agencies involved in a service user's care.

4. How to Contact Us About Data Protection

Our Data Protection Lead has day-to-day responsibility for data protection and privacy matters:

Organisation	Pringle's Care Services Limited
Email	monitoring@pringlescareservices.co.uk
Telephone	020 3743 7355
Address	Crown House, North Circular Road, Park Royal, London, NW10 7PN

You also have the right to complain to the Information Commissioner's Office (ICO) at any time – see Section 15. We would appreciate the opportunity to resolve your concerns first.

5. Our Role: When We Are a Controller and When We Are a Processor

Under Clause 24 (Data Protection) and Schedule 16 (Details of Provider Processing Activities) of the DPS Agreement, our role in relation to personal data shared with the Council depends on the type of data involved:

- **Joint Data Controller:** for "Shared Personal Data" — the personal data we and the Council both need in order to arrange and deliver care (e.g. service user demographic details, care needs, and next-of-kin information) — Pringle's and the Council act as joint controllers. We are jointly responsible for ensuring this data is processed lawfully, and we co-operate with the Council on data subject requests, notices to individuals, and record-keeping.
- **Data Processor:** for "Authority Data" — personal data provided to us by the Council which we process only on the Council's instructions (e.g. referral information, care package specifications, financial data relating to a service user's Council-funded care) — we act as the Council's processor and process this data strictly in line with the Council's written instructions and Schedule 16.
- **Independent Data Controller:** for personal data we hold about our own staff, and for service users whose care we provide independently of the Council (e.g. privately funded service users), we are the sole data controller.

For self-funding service users or those referred other than through the Council, Pringle's is the sole data controller of their personal data.

6. Personal Data We Collect About Service Users

To provide safe, high-quality care and to meet our obligations to the Council under the DPS Agreement, we may collect and hold the following categories of personal data about service users:

6.1 Identity and contact information

- Name, address, telephone number, and date of birth;
- Gender and, where provided, ethnicity;
- NHS number and GP details;
- Immigration/residency status where relevant to eligibility for services.

6.2 Care and health information

- Care and support needs assessments, risk assessments, and (where applicable) mental capacity assessments;
- Support plans, daily care logs, and records of care delivered (including via our Electronic Call Monitoring (ECM) system or manual timesheets where ECM does not apply);
- Health information, including medical history, diagnoses, medication administered or assisted with, and other health-related tasks identified in the support plan;
- Records of falls, accidents, incidents, and any follow-up risk assessments;
- Safeguarding concerns, referrals, and outcomes.

6.3 Relationships and representatives

- Name and contact details of next of kin, emergency contacts, and any person with legal responsibility for the service user (e.g. holder of a Lasting Power of Attorney);
- Name and contact details of other professionals involved in the service user's care (GP, social worker, community nurse, other providers).

6.4 Financial information (where we assist with finances)

- Records of any financial transactions we make on a service user's behalf, and of any assessed financial contribution due to the Council;
- Records relating to any reported financial irregularity or concern, in line with our safeguarding procedures.

6.5 Service delivery and quality records

- Complaints and compliments;
- Feedback from service user and family surveys;
- Records of cancelled calls, non-delivery of care, and related communications.

We do not require a Disclosure and Barring Service (DBS) check on service users; DBS information we hold relates only to our staff (Section 12).

7. Why We Collect This Data and Our Legal Basis for Using It

We only collect personal data that is necessary to provide safe, appropriate care and to meet our contractual and regulatory obligations. We rely on the following lawful bases under UK GDPR Article 6:

- Performance of a contract – to deliver the care and support services agreed in a service user's care/support plan, or under our contract of employment with staff;
- Legal obligation – to comply with CQC registration requirements, safeguarding law, employment law, and our obligations to the Council under the DPS Agreement;
- Vital interests – in an emergency, to protect a service user's life or immediate wellbeing;
- Legitimate interests – for day-to-day service administration, quality assurance, and audit, balanced against the individual's rights; and
- Consent – where we ask for and rely on explicit consent, for example for certain information sharing preferences or equality monitoring.

Because health information is “special category data” under Article 9 UK GDPR, we also rely on one of the following conditions: provision of health or social care (Article 9(2)(h)), the substantial public interest condition for social care purposes under Schedule 1 of the DPA 2018, or explicit consent. Safeguarding concerns are processed under the substantial public interest condition for safeguarding of individuals at risk (DPA 2018, Schedule 1, Part 2).

8. How and Why We Share Your Information

We may share service users' personal data with the following, always on a strictly need-to-know basis:

- The London Borough of Ealing (or other commissioning local authority) — for care management, funding, audit, and contract compliance, always via secure, encrypted systems as required by Schedule 7 of the DPS Agreement;
- GPs, community health teams, hospitals, and other health and social care professionals involved in the service user's care;
- Other care providers involved in a service user's package of care;
- The Care Quality Commission (CQC), for regulatory purposes;
- Emergency services, where necessary to protect life or safety;
- Safeguarding partners, where there is a safeguarding concern;
- Our professional advisers, auditors, and insurers, where necessary; and
- Any other party where we are required to do so by law or court order.

We will never sell personal data, and we do not share personal data with any third party for marketing purposes.

9. Information Sharing Protocol and Caldicott Principles

In line with Schedule 7 (Information Sharing Protocol) of the DPS Agreement and the Caldicott principles, we follow these safeguards whenever we share service user information with the Council and other partner agencies:

1. When we first assess a service user, we explain what information will be shared, with whom, and why, and we record that this explanation has been given.
2. Service users have the right to ask us to restrict the sharing of specific information. We will respect this wherever legally possible, and we record any such restriction clearly in the service user's file, including on the front sheet, together with the reasons.
3. Where there is a legal duty to share information even without consent — for example, where there is a serious risk to the health, safety, or welfare of the service user or others, or for the prevention, detection, or prosecution of a crime — we may do so, and we record the reason for the disclosure in the file.
4. Any transfer of information against a service user's stated wishes can only be authorised by the Council's authorised officer (or their deputy), consistent with the DPS Agreement.
5. Where a service user lacks capacity to decide about information sharing, we involve a carer or nominated advocate in line with the Mental Capacity Act 2005 and always act in the service user's best interests.
6. Secondary disclosure (sharing beyond Pringle's and the Council) requires permission from the originating organisation, except to protect safety and welfare, for legal proceedings, or for crime prevention/detection — and any such disclosure is recorded.
7. Where we receive a referral but are not selected to provide the service, we securely destroy or return all associated documentation without delay.

10. Your Rights

Under UK GDPR, you have the right to:

- Be informed about how your personal data is used (this Policy and our Privacy Promise);
- Access a copy of the personal data we hold about you (a “subject access request” or SAR);
- Have inaccurate personal data corrected, or incomplete data completed;
- Request erasure of your personal data in certain circumstances;
- Request that we restrict the processing of your personal data in certain circumstances;
- Object to processing based on legitimate interests;
- Request a portable copy of data you provided to us where processing is based on consent or contract and carried out by automated means; and
- Withdraw consent at any time, where consent is the basis for processing.

To make a request, contact our Data Protection Lead using the details in Section 4. We will need to verify your identity and may ask for proof of ID. We will respond within one calendar month, extendable by a further two months for complex requests. Where the personal data was shared jointly with, or provided by, the Council, we will liaise with the Council to fulfil requests relating to that data, as required under Clause 24 of the DPS Agreement.

11. Call Recording, Digital Tools and Meeting Notes

We may record telephone calls for training, quality monitoring, safeguarding, complaint handling, and record-keeping purposes. Where call recording is in operation, callers will be notified.

We may also make notes of meetings, assessments, and care reviews. Where we use digital tools to assist with notetaking or meeting summaries, this is done lawfully, and records are stored securely in accordance with our retention procedures (Section 14).

Where care hours commissioned exceed the threshold set by the Council (250+ hours per invoice period), we operate an Electronic Call Monitoring (ECM) system that records real-time call data (arrival/departure times, carer identity, and location) used for rostering and accurate invoicing. Below this threshold we maintain signed manual timesheets confirming actual call start and end times. ECM and timesheet data is stored securely and made available to the Council for audit and contract compliance purposes.

12. If You Work for Pringle's Care Services Limited

If you are an employee, worker, or contractor, we may collect the following personal information:

- Your name, address, phone number, and email address;
- Date of birth;
- Gender;
- National Insurance number;
- Bank details;
- Tax and payroll information;
- Emergency contact details;
- Right to work documentation;
- Employment contract details;
- Qualifications, training, skills, and work history;
- References;
- Details of leave, sickness, disciplinary matters, grievances, and performance;
- Driving licence and vehicle documentation where relevant to your role, including confirmation of appropriate business-use motor insurance where you use your own vehicle to transport service users;
- DBS check information where required;
- Health information, including occupational health information and fit notes;
- Equality monitoring information where voluntarily provided; and
- Records confirming completion of data protection, confidentiality, and safeguarding training, and signed confidentiality undertakings where required.

Where the Council transfers staffing information to us (or we transfer it to a replacement provider) in connection with a change of contract under TUPE, this is handled strictly in accordance with the Data Protection Legislation, as required by Schedule 9 of the DPS Agreement.

13. How We Keep Your Information Secure

We maintain appropriate technical and organisational measures to protect personal data against accidental loss, destruction, damage, alteration, or unauthorised disclosure, including:

- Registration with, and use of, the NHS-led Data Security and Protection Toolkit (DSPT), as required within three months of joining the DPS and reviewed/submitted at least annually;
- Secure, encrypted systems for all electronic correspondence and data exchange with the Council and other partner agencies;
- Access controls that limit staff access to personal data strictly to what is needed for their role;
- Confidentiality training for all staff, with signed confidentiality undertakings where required;
- Secure physical storage of paper records (e.g. locked cabinets) and secure electronic storage with password protection;
- Regular review of our policies and procedures in line with current statutory requirements and CQC and ICO best practice guidance; and
- Spot checks and an annual audit of any records relating to service user finances that we help manage.

All personnel involved in processing shared personal data are informed of its confidential nature, are subject to binding confidentiality obligations, and have undertaken adequate training in handling this data, in line with Clause 24 of the DPS Agreement.

14. How Long We Keep Your Information

We keep personal data only for as long as necessary for the purposes it was collected, and in line with our contractual obligations to the Council:

- Contract, care, and financial records connected with the DPS Agreement are kept for twelve (12) years after the Agreement (or the relevant individual placement agreement) has expired, in accordance with Clause 22 of the DPS Agreement;
- Referral documentation for service users we were not selected to support is destroyed or returned to the Council immediately once we are notified, we were unsuccessful;
- On termination or expiry of the DPS Agreement, any Council data in our possession is destroyed or returned to the Council within thirty (30) working days, unless a different retention period is agreed or required by law;
- Staff records are retained in line with employment law requirements and our internal HR retention schedule; and
- Where no other retention period applies, we follow best-practice retention guidance for health and social care records and our own records-management procedures.

Personal data is destroyed or disposed of securely (e.g. secure shredding of paper records and secure deletion of electronic records) once retention periods have expired.

15. Reporting Data Breaches

We take data security extremely seriously. If we become aware of a personal data breach (including a near miss), we will:

- Investigate and take immediate steps to contain and mitigate the breach;
- Notify the Council in writing within 24 hours of becoming aware of any breach affecting Shared Personal Data, and within 48 hours in relation to Authority Data, providing full details including categories and approximate numbers of individuals and records affected, as required by Clause 24 of the DPS Agreement;
- Notify the Information Commissioner's Office (ICO) within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms;
- Notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms; and
- Record the breach, our response, and any lessons learned, to prevent similar incidents recurring.

You can report a suspected breach, or any concern about how your information has been handled, to our Data Protection Lead using the details in Section 4.

16. International Data Transfers

We do not transfer personal data outside the United Kingdom or the European Economic Area. Where, exceptionally, an international transfer of Shared Personal Data or Authority Data is required, we will not do so without the Council's prior written consent (or, for data we control independently, without appropriate safeguards recognised under UK GDPR), in line with Clause 24 of the DPS Agreement.

17. Sub-Contractors and Other Data Processors

We do not engage any sub-contractor to process Authority Data or Shared Personal Data without the Council's prior written consent. Where we do engage a sub-contractor or third-party processor (for example, a payroll provider or an ECM software provider), we ensure that equivalent data protection obligations to those in this Policy and in Clause 24 of the DPS Agreement are included in our contract with them, and we remain fully responsible for their compliance.

18. Automated Decision-Making

We do not use automated processing to make decisions about service users or staff that would have a significant effect on them, without the Council's prior written consent (where relevant) and appropriate safeguards, in line with Clause 24.6 of the DPS Agreement.

19. Freedom of Information

The Council is subject to the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations. Where the Council needs our assistance to respond to a request for information, we will transfer any relevant request to the Council within two working days of receiving it, and provide any information the Council requires (in the format requested) within five working days, or such other period as the Council specifies, in accordance with Clause 25 of the DPS Agreement. We do not respond directly to Freedom of Information requests unless expressly authorised to do so by the Council.

20. Records We Maintain

To meet our contractual and regulatory obligations, we maintain (and make available to the Council on request) the following categories of records:

- Service user support plans;
- Service user daily logs (digital and/or paper);
- Assessments, risk assessments, and capacity assessments;
- Records of assistance with, or administration of, medication or other health-related tasks;
- Reports prepared for service user reviews;
- Health and safety audit reports;
- Staff rosters;
- Details of all staff employed and staff changes (starters and leavers);
- Staff records, including training and induction records;
- Records of accidents/incidents involving staff or service users, and any follow-up actions; and
- Complaints (and compliments) register.

21. Staff Training and Responsibilities

All staff receive data protection, confidentiality, and information-sharing training as part of induction, and refresher training thereafter. Staff are required to sign an agreement confirming they have received, read, and understood their responsibilities in relation to data protection and confidentiality, in line with Schedule 7 of the DPS Agreement. Staff who breach these responsibilities may be subject to disciplinary action under our disciplinary procedures.

22. Complaints

If you are unhappy with how we have handled your personal data, please contact our Data Protection Lead in the first instance (Section 4), so we can try to resolve your concerns directly.

You also have the right to make a complaint to the Information Commissioner's Office (ICO), the UK's independent regulator for data protection:

Website: ico.org.uk — Telephone: 0303 123 1113 — Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

23. Changes to This Policy

We review this Policy at least annually, and sooner if there is a change in law, ICO guidance, or the terms of the DPS Agreement (or any equivalent contract). When we update this Policy, we will update the effective date below and notify staff and service users of any significant change.

Effective date	01 July 2026
Last reviewed	01 July 2026

This Privacy Policy should be read alongside our Privacy Promise (our short public-facing summary) and is designed to demonstrate full compliance with Schedule 7 (Information Sharing Protocol) and Clause 24 (Data Protection) of the Ealing Council Community Services DPS Agreement,.