Data Protection and Data Security Policy V2025.2

This policy forms part of our statutory compliance framework and is read alongside: Safer Recruitment Policy, Confidentiality Policy, Information Governance Handbook, and Incident/Breach Procedure

Version Control

Date	New Version #	Made by	Details	Review Date
18/12/2023	V2023.1	Rhiannon Williams	Initial Policy	18/12/2025
18/11/2025	V2025.2	Rhiannon Williams	Review of policy and update in line with NHS COP	18/11/2026

City Care Southwest Ltd (the Employer) is committed to ensuring that all personal data handled by us will be processed according to legally compliant standards of data protection and data security.

Statement and purpose of policy

City Care Southwest Ltd is committed to ensuring that all personal and sensitive data handled by the organisation, whether relating to clients, staff, or other third parties, is collected, processed, stored, and disposed of in accordance with **UK GDPR, the Data Protection Act 2018, and all relevant regulatory guidance** (CQC for adults, OFSTED for children). We recognise our duty to protect the rights, privacy, and confidentiality of all individuals whose data we hold. This policy protects service users by ensuring their personal and sensitive information is collected, processed, and stored securely, reducing the risk of misuse, accidental disclosure, or regulatory breaches.

The purpose of this policy is to:

1. **Inform staff** of the types of personal information that may be held and how it is used.
2. **Set out clear rules** for the collection, storage, processing, sharing, and disposal of personal data, ensuring compliance with legal requirements.
3. **Clarify responsibilities** of staff, managers, DPOs, and the SIRO in relation to data protection and security.
4. **Provide guidance** on handling personal data securely in daily operations, including BYOD, shared office environments, and messaging systems.
5. **Mitigate risks** to individuals and the organisation, including unauthorized access, accidental disclosure, data loss, and regulatory non-compliance.
6. **Support operational and regulatory compliance**, including inspections by CQC, OFSTED, and DSPT audits.

This policy applies to all staff, including employees, directors, officers, consultants, contractors, casual or agency staff, trainees, homeworkers, and volunteers, across **Adult and Children's services**. It covers all personal data held electronically or on paper, in cloud-based systems, and any BYOD devices used for work purposes.

Risks mitigated:

- Regulatory breaches (GDPR, DPA 2018, CQC, OFSTED)
- Accidental or deliberate disclosure of client or staff data
- Loss or corruption of personal data
- Operational errors due to unclear roles or procedures

UK GDPR Articles 5 & 6, DPA 2018, DSPT, CQC Fundamental Standards, OFSTED Safeguarding Guidance

Definitions

Criminal records data means information about an individual's criminal convictions, offences, or alleged offences, and information relating to criminal investigations or proceedings.
Data protection laws mean all applicable laws relating to the processing of personal data, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
Data subject means the individual to whom the personal data relates.
Personal data means any information relating to an identified or identifiable natural person (data subject), directly or indirectly.
Processing means any operation or set of operations performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.
Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, health data, sex life, or sexual orientation.
Data Controller - The organisation or individual who determines the purposes and means of processing personal data.
Data Processor - Any person or organisation that processes data on behalf of the Data Controller.

Roles and Responsibilities

Role	Responsibilities	Notes
Rhiannon Williams DPO / IG Lead Adults	Oversee adult data protection compliance, manage breaches, handle SARs, advise staff.	Full-time operational responsibility. Includes CQC and Caldicott Compliance
Claire Best DPO / IG Lead Children	Oversee children's data protection, compliance, safeguarding-related records, handle SARs, advise staff.	Includes OFSTED and Caldicott compliance
Tony Merrick SIRO	Strategic oversight of data risk, escalates significant risks to Board.	Primarily finance, not day-to-day operations.
Managers and Directors	Monitor compliance, enforce policy, implement audit recommendations	Responsible for teams' adherence
All Other Staff	Follow policies, report breaches, maintain confidentiality, comply with BYOD rules.	Includes all staff using personal phones.
Dan's Computer Services IT Support	Technical controls, secure configuration, recovery, encryption, system monitoring	Works with DPO for containment/remediation

City Care Southwest Ltd is ultimately accountable for compliance with UK GDPR and the Data Protection Act 2018. Responsibility for day-to-day data protection activities is delegated to the DPOs; however, overall accountability remains with the organisation and its directors. Directors step in for high-risk ICO-reportable breaches or where escalation beyond DPO/SIRO is required.

Responsibilities per scenario:

- **Breach**: Staff → DPO → SIRO → Board; IT for technical fixes.
- **SAR**: Staff → DPO → SIRO; response within 28 days (or 3 months for complex requests).
- **Data sharing**: Staff → DPO approval → secure transfer / DSA in place.

If DPO is unavailable, the other DPO or SIRO assumes responsibility

Risks mitigated: accountability gaps, mismanagement, delayed breach response.
References: GDPR Articles 37–39, DSPT, CQC Regulation 17.

Data Protection Principles

All staff whose work involves using personal data must comply with the following principles. These principles guide how we handle data day-to-day and the risks they mitigate:

Lawful, Fair, and Transparent Processing

- Personal data is processed only where there is a lawful basis (e.g., contract performance, legal obligation, or legitimate interest).
- Data subjects are informed about how their data is used.

Risk mitigated: GDPR breach, loss of trust, legal penalties.

Purpose Limitation

Data is collected only for specific, explicit, and legitimate purposes, such as care delivery, HR, training, or safeguarding.

Our lawful bases for processing include:

- Legal obligation (safeguarding, CQC/OFSTED compliance)
- Contract (delivery of care and employment duties)
- Legitimate interests (service improvement, business operations)
- Consent (photos of clients for non-care purposes, marketing)
- Vital interests (life-saving situations)
- Public task where applicable (children's safeguarding functions)

Risk mitigated: Data misuse, regulatory non-compliance.

Data Minimisation

- Only data necessary for the intended purpose is collected and processed.
- Unnecessary or irrelevant data is not collected.

Risk mitigated: Exposure of excessive data, reputational and regulatory risks.

Accuracy

- Reasonable steps are taken to ensure data is accurate and up-to-date.
- Regular checks of client records, staff files, and system information.
- Staff must notify the DPO of inaccuracies for correction.

Risk mitigated: Decisions made on inaccurate data, harm to clients/staff.

Storage Limitation

- Data is retained only for as long as necessary according to retention schedules.
- Secure deletion or anonymisation is carried out at the end of the retention period.

Risk mitigated: Excessive retention, non-compliance, data breach exposure.

Integrity and Confidentiality (Security)

- Data is protected with appropriate technical and organisational measures: encryption, role-based access, strong passwords, multi-factor authentication, locked storage for physical files.
- BYOD staff devices must comply with security requirements.

Risk mitigated: Unauthorized access, data loss, accidental disclosure.

Accountability

- All staff are responsible for following the policy; managers ensure compliance in their teams.
- Data Protection Officers (DPOs) oversee and provide guidance.

Examples of Lawful Bases

- Contract: Delivering care services and staff employment duties.
- Legal obligation: Safeguarding, CQC/OFSTED compliance.
- Legitimate interests: Service improvement, operational monitoring.
- Consent: Marketing or client photographs.
- Vital interests: Life-saving interventions.
- Public task: Children's safeguarding functions.

Processing in children's homes aligns with OFSTED, SEND, KCSIE, and safeguarding requirements

Risk mitigated: Organisational failure to comply, regulatory fines.

Accessible Information & Communication Needs

City Care Southwest Ltd is committed to ensuring that all clients and children in our care can access and understand information relating to their care, treatment, and services. The Accessible Information Standard applies only to adults; however, Children's Services apply equivalent principles under OFSTED, SEND Code of Practice, and Children Acts 1989/2004. AIS and equivalent children's communication records are audited/reviewed at least annually to ensure compliance and accuracy.

Adults – Accessible Information Standard (AIS)

- We identify whether adults have any information or communication needs (ICN) at first contact.
- ICNs are recorded in Birdie to ensure they are available to all staff delivering care.
- Information provided (care plans, letters, consent forms) is adapted to meet the client's needs, e.g., large print, braille, easy-read, audio, or translated materials.
- Staff communicate appropriately during visits, phone calls, or emails, ensuring clients fully understand information provided.

Risks mitigated: Misunderstanding instructions, poor care outcomes, safeguarding issues, non-compliance with statutory requirements.

Children – Residential Care & Communication Needs

- Communication needs are identified at admission and recorded in ClearCare or OneDrive, in line with SEND Code of Practice (2015), Children Act 1989 & 2004, and Ofsted guidance.
- Materials and explanations are adapted to the child's needs, using visual aids, easy-read formats, or support staff where necessary.
- Staff are trained to ensure children can understand and express themselves about their care and welfare.
- Communication needs are reviewed regularly, especially if the child's circumstances or abilities change.

Risks mitigated: Miscommunication, poor engagement, safeguarding concerns, inspection non-compliance.

Confidentiality

Staff must maintain strict confidentiality of all personal and sensitive data.

- Discuss client information only in private rooms or using initials in open areas.
- Paper documents are locked; digital files are password-protected, encrypted, and accessed only by authorised staff.
- BYOD devices (personal phones, tablets, laptops) must not store client-identifiable data. Use PIN/password, biometric lock, MFA.
- Shared office precautions: conversations not overheard, printers/scanners used securely, cache cleared, separate networks from other business tenants.
- Report any actual or suspected breaches immediately to the relevant DPO.
- All communications (email, messaging apps, Birdie, Teams) must be secure, minimising client-identifiable data.
- Handle electronic and physical information securely when travelling or visiting clients.
- Staff must not discuss client or child information with friends, family members, partners, or any person outside the organisation.
- Staff must use headphones during Teams calls in shared or open office spaces
- Email auto-complete must be used cautiously to avoid accidental disclosure of client/staff data.

Data is shared externally only where legally permitted and necessary (e.g., GP, social worker, local authority, emergency services, Highfield, Achievement Training, payroll, DBS, regulators). All sharing is approved by a DPO, and a Data Sharing Agreement (DSA) is used where appropriate. Information is transmitted securely via encrypted email or secure portals. Dan's Computer Services holds controlled administrator access to Microsoft 365 for technical support only. Access is logged, monitored, and reviewed by the DPO and SIRO. **Risks mitigated:** Accidental disclosure, unauthorised access, reputational damage, regulatory non-compliance.

Breach Response

City Care Southwest Ltd takes all personal data breaches seriously. A breach includes unauthorised access, accidental loss, destruction, or disclosure of personal or sensitive data. Failure to report a breach is considered a disciplinary matter. An annual review of breaches is conducted as part of DPST compliance.

Immediate Actions

1) Staff discovering a breach must:
   a) Report immediately to the relevant DPO (Rhiannon for Adults, Claire for Children). Within 1 hour of discovery.
   b) Include date/time of breach, location, systems involved, and a brief description of the incident.
   c) Take any immediate steps to contain the breach, e.g., lock affected devices, change passwords, or remove physical documents from public access.

Responsibility: All staff

DPO Actions

2) DPO receives breach report:
   a) Log the breach in the Breach Register.
   b) Conduct an initial assessment of the breach to determine:
      i) Data types involved (personal/special category).
      ii) Number of individuals affected.

iii) Potential impact on data subjects.
iv) Whether the breach is high risk requiring notification to regulators.

c) Notify the SIRO (Tony Merrick) if the breach is significant or high-risk.

Responsibility: Rhiannon (Adults) / Claire (Children)

Containment & Remediation

3) Containment:
   a) Isolate affected systems or devices.
   b) Secure or retrieve lost paper records.
   c) Change access credentials if unauthorised access is suspected.

4) Remediation:
   a) Restore data from secure backups if appropriate.
   b) Apply software or system fixes to prevent recurrence.
   c) Retrain staff involved if the breach was caused by human error.

Responsibility: IT Support (Dan's Computer Services) for technical containment; DPO coordinates remediation with SIRO and relevant managers.

Notification

5) Regulatory Notification:
   a) If the breach poses a high risk to data subjects, the DPO must notify the ICO within 72 hours.
   b) The notification includes:
      i) Description of breach
      ii) Categories and number of data subjects affected
      iii) Likely consequences
      iv) Measures taken to mitigate risk
   c) If necessary, affected individuals are informed without undue delay.

Responsibility: DPO coordinates notification; SIRO informed; CEO/Directors may approve external communications.

Investigation & Reporting

6) Investigation:
   a) DPO conducts a full root-cause analysis.
   b) Determines whether policy, training, or systems need updating.
   c) Prepares a post-breach report summarising actions taken, lessons learned, and recommended changes.
7) Reporting:
   a) Report findings to SIRO and Board.
   b) Update the Breach Register with outcomes and closure details.

Responsibility: DPO leads; SIRO approves; relevant managers implement recommendations.

Training & Prevention

City Care Southwest Ltd links staff supervision and competency assessments directly to information governance and data protection training. All staff undergo regular one-to-one supervision where adherence to GDPR, DPA 2018, and organisational data protection policies is reviewed. Competency assessments include evaluation of secure

handling of client and staff information, safe use of BYOD devices, secure communication practices, and understanding of breach reporting procedures. Evidence of supervision and competency is recorded and maintained in staff records, supporting CQC inspections and demonstrating ongoing compliance with data protection and safeguarding standards. All staff receive refresher training on breach identification, reporting, and mitigation. Lessons learned are integrated into policy updates, staff briefings, and system safeguards.

Systems and Data Storage

City Care Southwest Ltd uses a range of systems and storage methods to manage personal and sensitive data for both Adults and Children's services. This section explains what each system is used for and how it supports secure data handling. Systems are UK/EU hosted and GDPR compliant. Back ups are performed according to vendor policies and data residency requirements.

Adults Services

- Birdie – Used for care management, rostering, client messaging, and photo documentation. Data is securely stored in the cloud; no local copies are kept on staff devices.
- Orta – Onboarding and staff HR documents (references, contracts, safer recruitment records). Centralised storage with access for authorised staff only.
- Hive & Highfield – Staff training records, qualifications, and learning management. Maintains evidence of competence and compliance.
- Microsoft 365 / OneDrive – Email communication and secure document storage, with controlled access and encryption.
- WhatsApp – Used for operational updates, client references only with initials. Adult carers may use their own devices, following policy rules for data protection and secure communication.

Children's Services

- ClearCare – Client records, care plans, and internal messaging.
- Teams (BYOD) – Staff communication, meetings, and messaging; no child-identifiable data stored locally.
- Training Hub / People Cloud – Staff training records and compliance monitoring.
- OneDrive – Scanned documents and secure storage with role-based access.
- Paper files – Stored in locked cabinets; restricted access.

BYOD / Staff Devices

- Adult carers and children's staff may use personal devices for work purposes.
- No client-identifiable data is stored locally on personal devices.
- Devices must be PIN/password-protected, encrypted where possible, and reported immediately if lost.

Shared Office Measures

City Care Southwest Ltd shares an office space with another business (City Security). Because of this, enhanced confidentiality and physical security measures are in place to ensure that no unauthorised person can access or view personal data belonging to clients or staff.

Physical Controls

Locked storage: Any paper documents (Adults rarely, Children's where applicable) are *always* kept in locked cabinets. Keys are held only by authorised staff.

Clear desk policy: Staff must ensure that no client or staff data is left on desks, whiteboards, printers, or visible workspaces when not in immediate use.

Secure printing: Staff must collect printed documents immediately. Printers must not store retained copies, and staff must check trays for stray pages.

Visitor awareness: External visitors (including City Security staff) must not be able to see client or staff data on screens or desks.

Conversations & Discussions

All client-related discussions must take place in a private room. If urgent discussion is required in a shared area, staff must use initials only or anonymised descriptors. Sensitive discussions (e.g., safeguarding, HR matters, concerns) must *always* take place behind closed doors.

Digital Protections in Shared Office

Staff must lock their screens whenever stepping away. Devices must be configured so screens cannot be viewed by others (privacy filters recommended for laptops). Wi-Fi networks must be password-protected and segregated if appropriate.

Communication and Messaging

City Care Southwest Ltd uses multiple communication channels to support service delivery and staff coordination. All staff must follow strict rules to ensure data is communicated securely and only when necessary.

Approved Communication Methods

- Microsoft Outlook / Teams for internal and external communication.
- Birdie messaging (BYOD) for Adults — secure in-app communication.
- Teams (BYOD) for Children's service communication.
- WhatsApp *for Adults only* to share operational information using non-identifiable data (initials only).
- Phone calls when sensitive information is required — not messages.

Prohibited Practices

- Sharing full client names on WhatsApp or SMS.
- Storing any client information on personal devices.
- Discussing client details in public or non-secure environments.
- Screenshots of system data being shared through any messaging app.

Messaging Security Rules

- Always minimise personal data — use initials, care plan numbers, or anonymised info unless absolutely necessary.
- Use Birdie or Teams for messages containing any identifiable information.
- Staff must report accidental disclosures immediately.
- Staff are aware that messages may be backed up to Apple/Google cloud; client-identifiable information must not be sent

Training and Staff Records

City Care Southwest Ltd maintains detailed records of staff training, competencies, safer recruitment documentation, and performance monitoring.

Adults Services

- Orta for HR files and safer recruitment documentation.
- Hive / Birdie for training records, certificates, and competency evidence.

Children's Services

- Orta for HR and staff compliance tracking.
- Training Hub for learning management and competency training.
- Paper staff files (where used) stored securely in locked cabinets.

Access Control

- Access is strictly role-based:
    - Registered Managers
    - DPO(s)
    - HR Administrators
    - Directors (where appropriate)

Staff do not have access to other staff's HR files.

Training Requirements

- Mandatory IG (Information Governance) training on induction.
- Annual refresher training for:
    - GDPR/DPA 2018
    - Confidentiality
    - Cybersecurity
    - Safe device use / BYOD
    - Secure communication
    - Recognising and reporting data breaches

Individual Rights

Under GDPR and DPA 2018, every data subject has specific rights regarding their personal data. City Care Southwest Ltd must respond fairly, transparently, and within legal timescales.

Key Rights

1. Right of access (Subject Access Request – SAR)
2. Right to rectification
3. Right to erasure (with exemptions in care settings)
4. Right to restrict processing
5. Right to data portability (rare in care)
6. Right to object
7. Rights relating to automated decision-making (not used here)

How Requests Are Handled

All requests must be forwarded immediately to the relevant DPO (Adults: Rhiannon Williams; Children's: Claire Best). The timescale is one calendar month unless extended due to complexity.

- Identity checks are always required before releasing data.
- Care records may not be erased where legal or safeguarding responsibilities apply.
- Requests are logged in the Individual Rights Register.

Criminal records information

Criminal records information will be processed in accordance with our safer recruitment policy. City Care Southwest Ltd processes criminal records information (DBS checks, police disclosures, risk assessments) in accordance with the Data Protection Act 2018 (Schedule 1, Part 1) and our Safer Recruitment Policy.
Criminal records data is:

- collected only where legally required,
- stored securely in Orta / People Cloud / locked cabinets,
- accessed only by authorised staff,
- retained in line with statutory retention schedules, and
- subject to enhanced confidentiality safeguards.

Data Retention Schedules

Audit outcomes and retention compliance are shared with staff during meetings and training sessions. Access to retained records follows the principle of least privilege; only staff with a legitimate need may view sensitive data.

Adult Care Records

Record Type	Description	Minimum Retention	Compliance Source
Adult Care Records (digital & paper)	Care plans, daily notes, assessments, risk assessments, reviews, rotas if linked to care.	8 years from date care ends	NHS Code of Practice (Adult Social Care)
Safeguarding Records (Adults)	Internal/external referrals, meeting minutes, outcomes	8 years after closure	NHS Code of Practice (Adult Social Care)
Medication Administration Records (MAR)	Adults' MAR sheets, PRN protocols.	8 years	NHS Records Management Code of Practice; Digital Care Hub.
Mental Capacity & DoLS	Assessments, best-interest decisions.	8 years	NHS Records Management Code of Practice; MCA best practice.
Incident/Accident Reports	Falls, injuries, medication errors.	10 years	NHS Code of Practice
Serious Incidents	SI / RIDDOR / notifiable safety incidents.	20 years	NHS Code of Practice

Children's Care Records

Record Type	Description	Minimum Retention	Compliance Source
Children's Care Records (Looked After Children)	Care plans, daily notes, risk assessments, LAC reviews, case management records.	75 years from DOB	Children Act 1989; Ofsted Residential Regulations
Safeguarding Records	Internal/external referrals, strategy discussions, meeting minutes.	Until child's 75th birthday	Ofsted / Children Act
Children's Medical Records	Consent forms, health assessments, medication logs.	75 years from DOB	Ofsted Regulations
Incident/Restraint Records	Physical intervention logs, behaviour incidents.	75 years from DOB	Ofsted Regulations
Children's Complaints	Complaints made by children or on behalf of children.	75 years from DOB	Ofsted Regulations
Staff Logs in Children's Homes	Duty rotas, visitor logs.	15 years	Ofsted Regulations

HR and Staff Files

Record Type	Retention	Compliance
Staff HR File (general)	6 years after employment ends	Limitation Act
Safer Recruitment Records	Application, references, ID, right to work, contracts.	6 years
DBS Checks	Certificate *not kept*, only record of check.	6 months for certificate / 3–6 years for record of check
Training Records	Mandatory & specialist training.	6 years after employment ends
Supervision & Appraisal Records	Notes, performance documentation.	6 years
Disciplinary Records	Formal warnings, investigations.	6 years

Finance and Business Records

Record Type	Retention	Compliance
Payroll, PAYE & Pensions	6 years	HMRC
Invoices & Accounts	6 years	Companies Act
Contracts (business)	6 years after termination	Limitation Act
Insurance Policies	6 years after expiry	FCA
Accident Books (Adults)	3 years	RIDDOR
Accident Books (Children)	Until child is 21 (or 24 if linked to safeguarding)	Limitation Act (minors)

Data Protection and Information Governance

Record Type	Retention	Compliance
Data Breach Logs	6 years	ICO guidance
SAR / Individual Rights Requests	2 years	ICO
DSPT Documentation	3 years	NHS Digital
Audit Logs (system access)	2 years	NHS DSP Toolkit
CCTV (if used)	30 days (standard)	ICO

Health and Safety

Record Type	Retention	Compliance
RIDDOR Reports	3 years	HSE
H&S Risk Assessments	3 years	HSE
Fire Safety Logs	6 years	Fire Safety Order
Equipment Maintenance Records	6 years	HSE
Lone Worker Records	3 years	HSE

Training and Digital Platforms

System	Record Type	Retention
Birdie / ClearCare	Full case records	Follow Adult/Children retention rules above
Orta (HR Files)	HR documentation	6 years after termination
Hive / Training Hub	Training certificates/records	6 years
Teams / OneDrive	Operational data	Follow content retention category

Messaging and Communication

Record Type	Retention
WhatsApp messages (Adults – no identifiable data)	Not stored — delete immediately
Teams messages	Default 30 days, unless downloaded and stored in case records.
Emails (Outlook)	3 years, or filed into appropriate retention category.

Monitoring and Audit

City Care Southwest Ltd undertakes regular monitoring and auditing to ensure all data protection, confidentiality, and cybersecurity measures remain effective and compliant.

Monitoring Activities

- Access logs in Birdie, ClearCare, Teams, Orta, and Microsoft — reviewed regularly.
- System permission reviews every 6–12 months or when staff leave/roles change.
- Incident and breach logs reviewed monthly by the DPOs.
- Device compliance checks via Microsoft tenant (e.g., encryption, MFA, login history).

Audits

- Annual internal audit of data protection compliance.
- Quarterly checks on staff use of BYOD devices and messaging practices.
- DSPT annual submission audit (Adults).

- OFSTED compliance audit (Children's).
- Spot checks on:
    - Locked storage
    - Clear desk practices
    - Use of initials on WhatsApp
    - Screen locking
    - Conversations held in private spaces

Reporting

Audit findings are reviewed with:

- Directors
- SIRO (Tony Merrick)
- DPOs (Adults: Rhiannon; Children's: Claire)
- Registered Managers

Corrective actions are logged and tracked.

References

- UK GDPR
- Data Protection Act 2018
- DSPT Toolkit Guidance
- CQC Fundamental Standards (Regulation 17 – Good Governance)
- OFSTED Social Care and Residential Guidance, KCSIE
- Accessible Information Standard

This policy is reviewed annually or sooner if legislation, systems, or risks change