Data Protection and Information Governance Policy

The single Insight Care Group framework for personal data — what we hold, how we hold it, who can see it, who we share it with, what individuals can ask of us, and how we keep it safe

---

Applies to: Every Insight Care Group home and head office, every employee (employed, agency, bank, sessional, volunteer), every contractor, every processor acting on the Company's behalf (Sona, Nourish, Eploy, Emma AI, Camascope, Microsoft 365 tenant, professional advisers), every visitor, every placing authority and every other party who handles personal data of an ICG-placed child or an ICG worker — and every child placed with us and every staff member as data subjects in their own right

Owner: Director (Controller and Data Protection Officer) — with the Responsible Individual providing Reg 45 quality of care assurance over information governance, the Registered Manager owning operational compliance on site for child and home records, the HR Manager owning operational compliance for employee records, and named processors (Sona, Nourish, Eploy, Emma AI, Camascope and Microsoft 365 tenant) under documented data processing agreements

Review cycle: Annual at policy level; on every material change in legislation, ICO guidance or Company processing (new system, new processor, new processing activity, new home, new category of children); on every material data breach or near miss; on every Reg 45 RI audit finding affecting information governance

1. Introduction

Insight Care Group runs residential children's homes for children with learning disabilities, autism, complex behaviour, sensory and communication needs, attachment and trauma responses, and mental health needs. Every aspect of that work — admitting a child, planning their care, recording their day, supporting their education, working with their family and their placing authority, employing the staff who care for them — turns on personal data. The way the Company handles that data is part of the way it cares for the people whose data it is.

This policy is the single Insight Care Group framework for personal data. It replaces the standalone Data Protection / GDPR Policy, Subject Access Request Guidance, Confidentiality and Information Sharing Policy, and Information Access and Authorisation Policy on the master tracker, because the four cover the same statutory framework and the same Caldicott principles and read more coherently as one document.

Where another policy needs to address how personal data is processed in that specific activity — finance recording, safeguarding, medication administration, recruitment, surveillance — that policy cross-references this one for the framework rather than repeating it.

2. Statement of Intent

Insight Care Group is committed to processing personal data lawfully, fairly and transparently, in line with the UK GDPR, the Data Protection Act 2018, the Common Law duty of confidence, the Caldicott Principles, Working Together to Safeguard Children, and the Children's Homes (England) Regulations 2015. The Company will:

- hold personal data only where it has an identified lawful basis (Article 6 UK GDPR) and, for special-category data, an additional Article 9 condition;
- apply the Caldicott Principles to every information-sharing decision about a child placed with us or a worker employed by us;
- respect every data subject right under the UK GDPR — to be informed, to access, to rectification, to erasure, to restrict, to data portability, to object, and not to be subject to a decision made solely by automated means;
- limit access to personal data to those who need it for their role, through role-based access controls applied across Sona, Nourish, Eploy, Emma AI, Camascope, SharePoint and Microsoft 365 (Section 16);
- share information about a child where the law requires us to, where it is necessary to protect the child or another person, and where any of the seven golden rules and Working Together apply — and not share otherwise;
- investigate every personal data breach within 72 hours of becoming aware, notify the ICO under Article 33 where the threshold is met, and notify affected data subjects under Article 34 where the threshold is met;
- train every member of staff in data protection at induction, refresh that training annually, and brief every new processor and contractor on the Company's expectations.

3. Scope and Application

This policy applies:

- to every ICG home, the head office and any other ICG premises;
- to every employee (employed, agency, bank, sessional, volunteer), every contractor and every processor acting on the Company's behalf;

- to every category of personal data the Company processes — child records on Nourish, employee records on Sona, recruitment records on Eploy, medication records on Camascope, AI-mediated child records via Emma AI, finance records in Revolut Business and on SharePoint, communications in the Microsoft 365 tenant, hard-copy records in the home, recordings from CCTV or body-worn devices, and any other category whether digital or paper;
- around the clock, including out-of-hours work supervised by sleep-in and waking-night staff;
- to data subjects who are children we look after, the family members of those children, employees and prospective employees, visitors, placing-authority staff, professionals working alongside us, contractors, and any other identifiable living individual whose data is held.

4. Legal and Regulatory Framework

- UK General Data Protection Regulation (UK GDPR) — the primary instrument: the seven data protection principles (Article 5), lawful basis for processing (Article 6), special-category data (Article 9), criminal conviction and offences (Article 10), data subject rights (Articles 12-22), controller obligations (Articles 24-43), breach notification (Articles 33-34), DPO requirements (Articles 37-39).
- Data Protection Act 2018 (DPA 2018) — implements the UK GDPR and sets the framework for law enforcement processing and intelligence services processing; Schedule 1 sets out the substantial public interest conditions for special-category and criminal conviction data including safeguarding of children (paragraph 18).
- Children's Homes (England) Regulations 2015 — particularly Reg 12 (protection of children), Reg 33 (Employment of staff), Reg 36 (Children's case records); Reg 37 (Other records); Reg 38 (Storage of records etc.), Reg 40 (notifications), Reg 45 (Responsible Individual quality of care review).
- Guide to the Children's Homes Regulations including the Quality Standards — Version 1.17 FINAL. The DfE's authoritative interpretation of the Quality Standards. Particularly relevant: the Leadership and Management Standard (Reg 13) — the records framework that underpins safe practice.
- Common Law duty of confidence — every member of staff working with personal information has a duty to keep it confidential, with the conditions for disclosure set out in this policy. Common law, not codified.
- Caldicott Principles (eighth edition, 2020) — eight principles for using and sharing confidential information in health and care; the duty to share information can be as important as the duty to protect it.
- Working Together to Safeguard Children — always read the current edition; information sharing in safeguarding contexts.
- ICO Guidance:
    - Guide to UK GDPR
    - Children's Code (Age Appropriate Design Code)
    - Right of Access (Subject Access Request) guidance
    - Personal Data Breaches
    - Accountability Framework
- Mental Capacity Act 2005 — engaged for any child aged 16 or 17 (and as best practice for younger children) when consent or other decision-making under this policy is in question; supported decision-making and the s.4 best-interests checklist apply.

- Children Act 1989 (including s.3 parental responsibility and s.22 looked-after children duty) and the
  - Children Act 2004 (s.11 safeguarding duty on partner agencies).
- Care Standards Act 2000 — establishes the regulatory framework for children's homes that the CHR 2015 sit underneath.
- Human Rights Act 1998 — Article 8 (private and family life) — the lens through which the Company considers proportionality of any data processing.
- Freedom of Information Act 2000 — ICG is not a public authority under the Act; relevant only when responding to a placing authority's FOI obligations.
- Privacy and Electronic Communications Regulations 2003 (PECR) — direct marketing rules where engaged; cookie consent on any ICG website.
- Crime and Disorder Act 1998 — s.115 power for disclosure to or by police, local authorities and other partner bodies for crime and disorder reduction.
- Computer Misuse Act 1990 — criminal liability for unauthorised access to computer material; relevant to insider-threat and external-attack scenarios.
- Information and Records Management Society (IRMS) toolkit — informs ICG's retention schedule; the children's case file 75-years-from-date-of-birth retention is drawn from there.
- NCSC Cyber Essentials and the
  - NCSC Cyber Assessment Framework — technical security yardsticks engaged by the IT and Cybersecurity Policy (row 124).
- Equality Act 2010 — reasonable adjustments engaged where a data subject's disability affects how the Company communicates with them.

5. Definitions

Term	What it means at ICG
Personal data	Any information relating to an identified or identifiable living individual (Article 4(1) UK GDPR). Includes name, address, identifier on a system, IP address, photograph and any other information that singles out an individual.
Special-category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data, biometric data for unique identification, health data, data concerning sex life or sexual orientation (Article 9 UK GDPR). At ICG the most commonly processed special category is health data — every placed child has health data on Nourish and on Camascope.
Criminal conviction and offence data	Data relating to criminal convictions, offences and related security measures (Article 10 UK GDPR). ICG processes this for safer recruitment (DBS) and where a placed child's case engages it.
Data subject	The identified or identifiable individual whose data is being processed. At ICG the principal categories are: placed children, employees, prospective employees, family members of placed children, visitors and placing-authority staff.
Controller	The person who determines the purposes and means of processing personal data (Article 4(7)). ICG is the controller for the data it processes.
Processor	A person or organisation that processes personal data on behalf of the controller (Article 4(8)). ICG's named processors include Sona, Nourish,

Term	What it means at ICG
	Eploy, Emma AI, Camascope, Microsoft (M365 tenant), Revolut Business, the Company's external accountant and any external HR consultant.
Data Protection Officer (DPO)	The person responsible for monitoring compliance with the UK GDPR and acting as the ICO contact (Article 39). At ICG the Director is the DPO. The Company will appoint a separate or external DPO when scale, conflict of interest or ICO guidance requires it.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12)). Section 18 sets the response.
Pseudonymisation	Processing personal data so that it can no longer be attributed to a specific data subject without additional information held separately and subject to technical and organisational measures (Article 4(5)).
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes by which they signify agreement to the processing (Article 4(11)). Consent must be capable of being withdrawn as easily as it is given.

6. Roles and Responsibilities

Role	Responsibilities
Director (Controller and DPO)	Owns this policy. Acts as the Company's Data Protection Officer in the absence of an independent DPO appointment. Signs the Record of Processing Activity (Section 19) annually. Authorises every Data Processing Agreement (DPA) with every processor before processing starts. Approves every Data Protection Impact Assessment (DPIA) before the relevant processing starts. Decides every Article 33 ICO breach notification and every Article 34 data subject notification. Final decision-maker on every SAR refusal, fee, partial fulfilment or extension. Reviews this policy annually.
Responsible Individual (RI)	Reg 45 quality of care assurance over information governance — twice-yearly per-home audit including sample SARs (where any), sample access logs, sample sharing decisions, and the Information Asset Register. Escalates any concern to the Director and, where the threshold is met, to Ofsted under Reg 40 and to the ICO.
Registered Manager (RM)	Operational compliance on site for every child record and every home record. Owns the home's Information Asset Register (Section 19). Authorises and reviews per-staff Nourish access for staff in their home (joiners / movers / leavers — Section 16.4). Triages and escalates every personal data breach in their home within 24 hours of becoming aware (Section 18). Handles every Subject Access Request received at the home in first instance and forwards to the DPO same day (Section 14). Approves every information-sharing decision in their home at the seven-golden-rules level (Section 15).
HR Manager	Operational compliance for every employee record on Sona, Eploy, payroll and any other HR system. Authorises and reviews Sona, Eploy and payroll access (joiners / movers / leavers — Section 16.4). Triages and escalates every HR-record breach within 24 hours. Handles every employee SAR in first instance and forwards to the DPO same day. Acts as the senior decision-maker on confidentiality issues between an

Role	Responsibilities
	employee and the home where they choose to escalate over the RM.
Caldicott Guardian (informal at ICG)	A senior person responsible for protecting the confidentiality of information about people receiving care from ICG and enabling appropriate information sharing. At ICG the RI fulfils this function until the Company appoints a designated Caldicott Guardian; the function is named because it is recognised by placing authorities and by ICO.
Information Asset Owners (per system)	A named owner for each information asset (Sona — HR Manager; Nourish — RM per home; Eploy — HR Manager; Emma AI — Director; Camascope — RM per home; SharePoint home folders — RM; SharePoint head office — Director; Microsoft 365 tenant — Director). Each owner is responsible for the data held in their system, for the access list to their system and for the DPA covering it.
Senior staff and Shift Leaders	First-line application of role-based access (RBAC) on shift — confirm that only those who need to see a record are looking at it; remind colleagues of the seven golden rules in the moment.
All staff	Process personal data only as needed for the role and only by the routes this policy and the system-specific Standard Operating Procedures set. Report any suspected breach the same shift. Complete induction and annual data protection training.
Processors (Sona / Nourish / Eploy / Emma AI / Camascope / Microsoft 365 tenant / Revolut Business / accountant / external HR)	Process personal data only on documented instructions from the Director, under a current written Data Processing Agreement that satisfies Article 28 UK GDPR. Notify the Director of any personal data breach affecting ICG data within 24 hours of becoming aware. Permit and contribute to audits by the Director or RI as required.
Visitors and contractors	Sign in, sign confidentiality undertaking where required, follow staff direction on what they can see and what they cannot.
Children and young people, families and employees as data subjects	Are entitled to every data subject right under the UK GDPR (Section 13). The Company supports them to exercise those rights — including in age- and ability-appropriate ways for children and young people.

7. The Data We Hold

The Company holds personal data in the following principal categories. The full Record of Processing Activity at Section 19 documents the processing for each category.

Category of data subject	Categories of personal data held	Principal system
Placed children and young people	Identity, contact, school, family contact, education, health, behaviour, safeguarding, special-category health data, sometimes criminal-conviction data, photographs and videos in line with the Placement Plan consent, voice and AI-mediated summaries through Emma AI	Nourish, Camascope (medication), Emma AI, SharePoint home folder, hard-copy where required
Family members and significant others of placed children	Identity, contact, relationship, contact arrangements, safeguarding information, sometimes special-category data (e.g. health where relevant to contact decisions)	Nourish (linked to child record)
Employees and	Identity, contact, right to work, education and employment	Sona

Category of data subject	Categories of personal data held	Principal system
prospective employees	history, DBS, references, payroll, training, supervision, performance, disciplinary, health (sickness, occupational health), special-category data (sometimes), emergency contacts	(employee), Eploy (recruitment), Payroll
Agency, bank, contractors and volunteers	Identity, right to work, contracted scope, ID and DBS verification	Sona (engagement record), Eploy (where recruitment-led)
Placing authority staff and visiting professionals	Name, role, contact, communications about a child	Nourish (linked to child record), Microsoft 365 (correspondenc e)
Visitors at the home	Sign-in book / GEEP visitor information (cross-reference PEEP Policy)	Hard-copy sign-in + SharePoint home Fire Log
Other (CCTV, audio in vehicles, body-worn devices where engaged)	As recorded — covered by the relevant DPIA before any deployment	CCTV / body-worn device storage

8. Data Protection Principles (Article 5 UK GDPR)

The Company processes every personal data item against the seven UK GDPR principles. Every Standard Operating Procedure for handling personal data is designed against them; every DPIA tests them; every annual policy review revisits them.

Principle	How ICG applies it
Lawfulness, fairness and transparency (Art 5(1)(a))	Every processing activity has an identified Article 6 lawful basis (and where relevant an Article 9 condition); privacy notices written in clear plain English (age-appropriate for children) are provided to every data subject.
Purpose limitation (Art 5(1)(b))	Personal data is collected for the specific purpose recorded in the ROPA; reuse for a new purpose requires a fresh compatibility test or a new lawful basis.
Data minimisation (Art 5(1)(c))	The Company collects only what is needed for the recorded purpose. Mandatory fields on every form are tested against this principle at the annual review.
Accuracy (Art 5(1)(d))	Records are kept up to date — child records on every Placement Plan review, employee records on every annual cycle, system records on every Joiner-Mover-Leaver event. Data subjects have a right to rectification (Section 13.3).
Storage limitation (Art 5(1)(e))	Retention is set in the per-category schedule at Appendix H, with the children's case file at 75 years from date of birth.
Integrity and confidentiality (security) (Art 5(1)(f))	Technical and organisational measures at Section 17 — RBAC, encryption, MFA, transit security, hard-copy locked storage, secure

Principle	How ICG applies it
	destruction.
Accountability (Art 5(2))	The Company can demonstrate compliance through this policy, the ROPA, the DPIA log, the breach log, the training matrix on Sona, and the annual Director and RI audits.

9. Lawful Basis for Processing

Every processing activity at ICG has a documented Article 6 lawful basis recorded in the Record of Processing Activity (Section 19). The principal bases ICG relies on are:

- Article 6(1)(c) legal obligation — including CHR 2015 obligations to keep records, HMRC record-keeping, RIDDOR reporting and Reg 40 notifications;
- Article 6(1)(b) contract — for processing necessary to perform the employment contract;
- Article 6(1)(d) vital interests — engaged in critical incidents (cross-reference Business Continuity and Critical Incident Policy);
- Article 6(1)(e) public interest task — where ICG is acting in support of the placing authority's safeguarding duty;
- Article 6(1)(f) legitimate interests — for limited Company-administration processing (e.g. internal management reporting) where the data subject's rights and interests do not override the Company's interests; documented in a legitimate interests assessment in the ROPA;
- Article 6(1)(a) consent — used only where the law requires it (e.g. photographs / video / specific marketing in due course where the Company engages it) and only where the consent is freely given, specific, informed, unambiguous and can be withdrawn as easily as it was given.

For special-category data (UK GDPR Article 9 + DPA 2018 Schedule 1) the principal conditions ICG relies on are:

- Article 9(2)(b) — employment, social security and social protection law obligations and rights;
- Article 9(2)(c) — vital interests where the data subject is physically or legally incapable of giving consent;
- Article 9(2)(h) — provision of health or social care or treatment, the management of health or social care systems and services, with safeguards under DPA 2018 Schedule 1 paragraph 2;
- Article 9(2)(g) + DPA 2018 Schedule 1 paragraph 18 — substantial public interest condition for safeguarding of children and individuals at risk;
- Article 9(2)(f) — establishment, exercise or defence of legal claims.

For criminal conviction and offences data (UK GDPR Article 10 + DPA 2018 Schedule 1) ICG relies on the substantial public interest conditions in DPA 2018 Schedule 1 — in particular paragraph 6 (statutory etc and government purposes) and paragraph 18 (safeguarding) for child records, and paragraph 14 (preventing or detecting unlawful acts) and DBS-related conditions for employee records.

10. Children's Data and Mental Capacity

Every child placed with Insight Care Group has a learning disability and may also have autism, complex behaviour, sensory and communication needs, attachment and trauma

responses, and mental health needs. Children's personal data attracts specific protections, and the Company applies them as follows:

- ICO Children's Code (Age Appropriate Design Code) — applied to any digital service the Company uses where children are likely to access it as users; applied as best practice to the way the Company designs privacy notices for children.
- Privacy notices for children — written at the appropriate reading age, with symbol or pictorial versions where the child's communication profile requires.
- Mental Capacity Act 2005 — engaged for any child aged 16 or 17, and applied as best practice for younger children. The five statutory principles inform every decision under this policy involving the child's own data — including SARs, rectification requests, sharing decisions and consent. Where the child has capacity for the specific decision, the child's decision applies. Where the child lacks capacity for the specific decision, the s.4 best-interests checklist applies, recorded under the Mental Capacity Act framework on Nourish.
- Parental responsibility — under s.3 of the Children Act 1989, parental responsibility includes a right to make decisions on the child's behalf where the child does not have capacity. Where parental responsibility is shared (e.g. between two parents and the placing local authority under a care order), the Company identifies the holder(s) of parental responsibility and engages them in line with the Placement Plan.
- Gillick competence — for processing decisions about a child that the child themselves can take, the Company applies the Gillick competence test as informed by current best practice.
- Sharing with parents — limited to what the Placement Plan and any court order provide for; the Company does not share with a parent simply because they are a parent if the Placement Plan, the court order or the placing authority directs otherwise.

11. Privacy by Design and Default; DPIAs

Privacy by design and default (Article 25 UK GDPR) is built into every new processing activity at ICG before it goes live. The Company adopts the following discipline:

- a Data Protection Impact Assessment (DPIA) is completed for any new processing that is likely to result in a high risk to the rights and freedoms of natural persons — including any new system, any change to how a placed child's data is processed (e.g. introduction of CCTV, body-worn devices, Emma AI), any new processor, any large-scale processing of special-category data, any systematic monitoring;
- the DPIA template is at Appendix E. It is completed by the proposing Information Asset Owner and signed by the Director before processing starts;
- where the DPIA identifies a residual high risk that cannot be mitigated, the Director consults the ICO under Article 36 before processing starts;
- DPIAs are reviewed at least every two years and on any material change.

12. Data Subject Rights — Overview

Every data subject has the following rights under the UK GDPR. Section 13 sets out how ICG delivers each right. The Subject Access Request procedure (Section 13.2) is detailed separately at Section 14 because it is the right most frequently exercised.

Right	UK GDPR article	Engaged at ICG when
Right to be informed	Articles 13-14	Always — through privacy notices at the point of data collection.
Right of access (SAR)	Article 15	On request from any data subject.
Right to rectification	Article 16	On request where data is inaccurate or incomplete.
Right to erasure ("right to be forgotten")	Article 17	On request — limited by statutory retention obligations.
Right to restriction of processing	Article 18	On request — pending investigation of accuracy, lawfulness, etc.
Right to data portability	Article 20	On request — limited to processing based on consent or contract and carried out by automated means.
Right to object	Article 21	On request — particularly where the lawful basis is legitimate interests or public interest task.
Rights relating to automated decision-making, including profiling	Article 22	Where any decision is made solely by automated means; ICG does not currently make such decisions.

13. Data Subject Rights — Detail

13.1 Right to be informed

- Privacy notices are provided at the point of data collection — at admission for a placed child, at offer of employment for an employee, at first visit for a visitor, etc.
- Privacy notices set out: who the controller is and the DPO contact; the purposes and lawful basis for processing; categories of data; recipients; retention period; the data subject rights; the right to complain to the ICO.
- Notices are written in clear plain English; age-appropriate versions are available for children including symbol or pictorial versions where the child's communication profile requires.

13.2 Right of access — Subject Access Request (SAR)

Detailed SAR procedure at Section 14. Summary: every data subject may request a copy of the personal data the Company holds about them; the Company responds within one month, free of charge in most cases, after identity verification.

13.3 Right to rectification

- A data subject may ask the Company to rectify inaccurate personal data or complete incomplete data.
- Routine corrections to a child or employee record are made by the relevant Information Asset Owner on receipt of the request; complex corrections (where the accuracy is in dispute) are escalated to the Director.
- Acted on within one month of request (with up to two further months where necessary, with reasons given to the data subject).

- Where the Company has shared the data with third parties, the Company notifies them of the rectification where this is possible and would not involve disproportionate effort.

13.4 Right to erasure

- A data subject may ask the Company to erase personal data in specified circumstances (Article 17(1)).
- ICG refuses the request where erasure would conflict with a statutory retention obligation — including child record 75-year retention under the IRMS toolkit, HMRC business records 6-year retention, and any active case file engaged in safeguarding or in legal action. The Company explains the basis for the refusal to the data subject.
- Where erasure is required, the Company erases or anonymises the data and notifies third-party recipients where possible.

13.5 Right to restrict processing

- A data subject may ask the Company to restrict processing of their data in specified circumstances (Article 18(1)) — for example, while accuracy is being investigated.
- Restriction is implemented by suspending non-essential processing while the underlying issue is resolved.

13.6 Right to data portability

- Limited to processing based on consent or contract and carried out by automated means (Article 20).
- Where engaged, the Company provides the data subject's personal data in a structured, commonly used and machine-readable format.

13.7 Right to object

- A data subject may object to processing based on Article 6(1)(e) public interest task or Article 6(1)(f) legitimate interests (Article 21).
- The Company stops the processing unless it can demonstrate compelling legitimate grounds that override the data subject's interests, or the processing is for the establishment, exercise or defence of legal claims.

13.8 Automated decision-making

- ICG does not currently make any decision about a placed child or about an employee solely by automated means.
- Where Emma AI or any other AI-assisted tool is used, the output is reviewed by a member of staff before any decision is taken; the human element protects the data subject's rights under Article 22.

14. Subject Access Requests — Full Procedure

Every Subject Access Request is acknowledged within five working days and responded to in full within one month of the date of receipt (or of identity verification, where that took longer). The procedure has nine steps.

1. Receive — a SAR may be made verbally, in writing, by email to dpo@insightcare.uk, by Sona / Nourish message, by letter to the home or to head office, or by the SAR Form at Appendix B. The Company accepts a request in any form.

2. Acknowledge — the recipient (RM for child / home requests, HR Manager for employee requests) acknowledges within five working days and forwards to the DPO the same day. The acknowledgement does not need to confirm the Company will fulfil the request; it confirms receipt and what happens next.
3. Verify identity — the DPO confirms the identity of the requester, using a method proportionate to the data requested. For a current employee, Sona login is sufficient. For a member of the public, two pieces of ID (one photo) are typically requested. Where the requester is a third party acting on behalf of the data subject (e.g. parent on behalf of a placed child, solicitor on behalf of an employee), evidence of authority is required.
4. Apply Mental Capacity Act and Gillick competence — for any request relating to a placed child's data, the Company assesses whether the child has capacity for the specific decision and whether the request engages the s.4 best-interests checklist. The presumption is that the Company will respond directly to the child where the child has capacity for the request.
5. Scope and search — the DPO works with the relevant Information Asset Owner to identify the systems holding the requester's data (Nourish, Sona, Eploy, Camascope, Emma AI, SharePoint home folder, payroll, email) and run a reasonable and proportionate search.
6. Redact and apply exemptions — third-party personal data is redacted unless that party has consented or it is reasonable to disclose without their consent. Exemptions are applied where they engage — including the management information exemption (DPA 2018 Schedule 2 paragraph 7), references (DPA 2018 Schedule 2 paragraph 24), legal professional privilege, crime prevention and detection, and child / family / employment-related exemptions where they apply.
7. Compile and send — the Company provides the data in a commonly used electronic format unless the requester asks otherwise. The response includes: the data; confirmation of processing and the purposes; categories of data; recipients; retention; the data subject's further rights; the right to complain to the ICO. The response is sent securely (encrypted attachment, secure portal, recorded delivery for paper).
8. Time and fee — first response within one month of identity verification. Up to a further two months where the request is complex or numerous, with the data subject informed within the first month. No fee except where the request is manifestly unfounded or excessive (charged at the reasonable administrative cost) or where the requester asks for further copies of the same information.
9. Record and close — the SAR is logged on the SAR Register on Sona (date received, requester, date acknowledged, date verified, date responded, fee charged where any, exemptions applied where any, outcome, complaint to ICO where any). The Director audits the SAR Register quarterly.

Refusing a SAR — the Company refuses a SAR only where it is manifestly unfounded or excessive (recorded in writing with reasons), where it would adversely affect the rights and freedoms of others (e.g. would disclose another person's personal data without their consent or a basis to do so), or where an exemption applies. The data subject is informed of the refusal, the reasons, and their right to complain to the ICO.

15. Confidentiality and Information Sharing

A Common Law duty of confidence applies to every member of staff in respect of every piece of confidential information they encounter at work — personal information about a placed child, a family member, a colleague, a contractor, a placing-authority staff member. The duty sits alongside the UK GDPR; meeting the UK GDPR does not necessarily release a member of staff from the duty of confidence.

15.1 When information may be shared

Information about a child or an employee may be shared with a person or organisation outside ICG only where one or more of the following applies:

- the data subject (or a person with parental responsibility for them where the data subject does not have capacity) has consented;
- the law requires the disclosure — including statutory notification (Reg 40 Ofsted, RIDDOR HSE, Tax HMRC, LADO referral), a court order, a police request supported by a Crime and Disorder Act 1998 s.115 power, a placing-authority safeguarding request, or a coroner's request;
- the disclosure is necessary to protect the vital interests of the data subject or another person — for example, where a child is in immediate danger;
- the disclosure is necessary to safeguard a child (Working Together to Safeguard Children) or another vulnerable person;
- the disclosure is necessary for the establishment, exercise or defence of a legal claim;
- the disclosure is permitted under the Substantial Public Interest condition in DPA 2018 Schedule 1 (in particular paragraph 18 for safeguarding).

15.2 Caldicott Principles

Every information-sharing decision is tested against the eight Caldicott Principles:

- Justify the purpose(s) for using confidential information.
- Use confidential information only when it is necessary.
- Use the minimum necessary confidential information.
- Access to confidential information should be on a strict need-to-know basis.
- Everyone with access to confidential information should be aware of their responsibilities.
- Comply with the law.
- The duty to share information for individual care is as important as the duty to protect patient / client confidentiality.
- Inform individuals about how their confidential information is used and what choices are available.

15.3 Seven Golden Rules for Information Sharing

From the HM Government Information Sharing guidance and Working Together to Safeguard Children:

- Information sharing is necessary for the protection of a child where there are concerns that the child is suffering or at risk of suffering significant harm.
- Where possible, share with consent and respect the wishes of those who do not consent — but where there is reason to share without consent (safeguarding etc), do so.
- Consider safety and well-being — the safety of the child is paramount.
- Necessary, proportionate, relevant, adequate, accurate, timely and secure.
- Keep a record — every decision to share (and to not share) is recorded on Nourish with the reason.
- Seek advice — from the RM, the DPO, the Caldicott Guardian or the placing authority where the decision is finely balanced.

- Share information securely — by the right channel, with the right party, with the right safeguards.

15.4 Sharing with placing authorities and professionals

- Sharing with the placing authority's social worker, IRO and any other named professional is routine for the care of the child and is recorded on Nourish in the child's record.
- Sharing with other agencies (school, GP, mental-health team, therapist) follows the Placement Plan and is recorded.
- Sharing with non-public-sector bodies (private therapy, leisure providers) is by the parent / placing-authority arrangement and is recorded.

15.5 Sharing with parents and family

- Sharing follows the Placement Plan, the court order in place (if any), and any decision recorded by the placing authority about contact and information.
- The Company does not share with a parent or family member contrary to the Placement Plan; where a parent or family member asks for information the Placement Plan does not allow, the Company refers them to the placing authority.

15.6 Sharing with police and the criminal justice system

- Routine police requests for information (witness statements, body-worn footage, recordings) are met under DPA 2018 Schedule 2 Part 1 paragraph 2 (crime and taxation) where appropriate.
- Requests engaging serious safeguarding concerns are escalated to the Director and the placing authority.

16. Information Access and Authorisation

Access to personal data at ICG is granted on a strict need-to-know basis through role-based access controls (RBAC). Every system the Company uses operates under the same principles, with the system-specific implementation set in the system's own access matrix.

16.1 Principles

- Need-to-know — a member of staff has access only to the personal data they need to perform their role.
- Least privilege — access is set at the minimum level required and is increased only on a specific business need.
- Segregation of duties — sensitive decisions (e.g. payroll change + payment release) are split across roles.
- Joiner / Mover / Leaver — access is provisioned, reviewed and revoked in line with the JML procedure at Section 16.4.
- Logging — every access to a sensitive record is logged by the system; the Director and RI sample logs at the quarterly audit.

16.2 Access levels by role (typical)

The table below is the typical access pattern. The full per-system matrix is at Appendix D.

Role	Sona	Nourish (child + home)	Eploy	Camascope	Emma AI	SharePoint home	SharePoint head office	M365 tenant
Director	Full + admin	Full read; targeted write	Full + admin	Full read	Full + admin	Full	Full + admin	Global admin
Responsible Individual	Read (audit)	Full read; quarterly audit	Read (audit)	Read (audit)	Read (audit)	Full read	Read	Read
Registered Manager	Read for own home staff	Full for own home	Read for own home recruitment	Full for own home	Read for own home	Full for own home	Limited	Standard user
Deputy Manager	Limited (own role)	Full for own home	Limited	Full for own home	Read for own home	Full for own home	No	Standard user
Senior staff / Shift Leader	Own record	Own home — active children only	No	Own home medication round	Read	Own home	No	Standard user
Care staff (employed / bank)	Own record	Own home — active children only	No	Own home medication round	Read	Own home	No	Standard user
Agency / sessional / volunteers	Engagement record	Active shift child only — read only or limited write per RM authorisation	No	Own shift medication round only	No	Own shift home only	No	Guest user
HR Manager	Full + admin (HR)	No (unless investigating a staff matter)	Full + admin	No	No	No	Full HR folder	Standard user
Billing function	Read (payroll)	No	No	No	No	Read finance folder	Read	Standard user
Maintenance Officer	Own record	No	No	No	No	Limited (maintenance folder)	Read	Standard user

Where a specific situation requires access outside the typical pattern (e.g. an HR investigation needing access to a Nourish entry, a Maintenance Officer needing a particular SharePoint folder for a one-off task), the access is granted by the Information Asset Owner, time-limited, logged and revoked when no longer needed.

16.3 Joiner / Mover / Leaver (JML)

Every starter, internal mover and leaver triggers a JML check by the relevant Information Asset Owner.

1. Joiner — access provisioned only after offer accepted, contract signed and pre-employment checks (including DBS) cleared. Access set at the typical role level (Section 16.2). Induction completed before the first unsupervised shift includes data protection (Section 22).
2. Mover — access reviewed on every role change (promotion, transfer between homes, change of duties). Old role permissions revoked; new role permissions provisioned.
3. Leaver — access disabled on the last day of employment; Sona, Nourish, Eploy, Camascope, Emma AI, SharePoint and M365 accounts closed or transitioned within five working days of the leaving date; physical access (keys, fobs, badges) returned; Company devices returned and wiped per the IT and Cybersecurity Policy.

16.4 Audit

- Monthly — Information Asset Owners review their access list and confirm no inappropriate access.
- Quarterly — the Director reviews a sample of access logs across systems.
- Twice-yearly — the RI samples access as part of Reg 45.
- Annually — full access recertification by every Information Asset Owner — confirmation that every active user still requires their current access.

17. Data Security

- Technical measures — encryption in transit (TLS) and at rest for every system holding personal data; multi-factor authentication for every staff account on every system; password complexity and rotation in line with NCSC current guidance; managed devices on every laptop / tablet through the Microsoft 365 tenant; mobile device management on every Company-issued mobile.
- Organisational measures — access on a strict need-to-know basis (Section 16); training (Section 22); clear-desk policy in offices that hold hard-copy records; locked storage of any hard-copy record; visitor sign-in.
- Hard-copy records — kept to a minimum; where held, kept in locked storage; transported only by secure means (encrypted media, sealed envelope for short journeys); never left unattended in a vehicle.
- Secure destruction — paper shredded to BS EN 15713 (or equivalent); electronic media wiped to NIST SP 800-88 standard or physically destroyed; certificates of destruction retained for 6 years.
- Off-site working — staff working from home or from another home are reminded of the need to protect screens from view, to lock devices when leaving them, and to follow the Use of Personal Mobile Devices Policy.
- Detail at the technical and operational level lives in the IT and Cybersecurity Policy.

18. Personal Data Breach Procedure

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include: a lost laptop or paper file; an email sent to the wrong recipient; a

successful phishing attack; a ransomware infection; a hostile login; a Nourish record updated by mistake; a placing authority sent another child's records.

1. Detect and contain — the staff member who detects the breach tells the RM (for home-record breaches) or the HR Manager (for employee-record breaches) the same shift. The Information Asset Owner takes immediate containment action (recall the email, freeze the account, isolate the device).
2. Notify the DPO within 24 hours of detection. The DPO opens a Breach Record on Sona (the template at Appendix F).
3. Assess the risk to the rights and freedoms of the data subjects affected — including the nature, categories and approximate number of personal data records concerned; the likely consequences; the measures taken or proposed to address the breach and mitigate possible adverse effects.
4. Notify the ICO under Article 33 UK GDPR within 72 hours of becoming aware of the breach, where there is a risk to the rights and freedoms of natural persons. Where the 72-hour deadline cannot be met, the notification is made later with reasons for the delay.
5. Notify affected data subjects under Article 34 UK GDPR without undue delay, where the breach is likely to result in a high risk to their rights and freedoms — unless one of the exceptions applies (data was encrypted, subsequent measures eliminated the risk, or it would involve disproportionate effort).
6. Notify the placing authority and (where the breach engages a child's safeguarding) the LADO. Notify Ofsted under Reg 40 where the threshold is met. Notify the police where a criminal offence is suspected.
7. Investigate and learn — within 28 days of close-out, the Director and the RI conduct a learning review; lessons feed into this policy, the IT and Cybersecurity Policy, the relevant SOP and the training plan.

Near misses — any incident that did not result in a breach but could have done is also recorded on the Breach Record and reviewed; near misses are the cheapest learning the Company gets.

19. Record of Processing Activity (ROPA)

The Company maintains a Record of Processing Activity under Article 30 UK GDPR. The ROPA records, for every processing activity:

- the name and contact details of the Controller (ICG) and the DPO (Director);
- the purpose(s) of the processing;
- the categories of data subjects and the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed (including processors and third countries / international organisations where applicable);
- the retention period (cross-reference Appendix H);
- the lawful basis under Article 6, and where applicable the special-category condition under Article 9 + DPA 2018 Schedule 1;
- a general description of the technical and organisational security measures applied;
- where applicable, a reference to the Legitimate Interests Assessment (LIA) or Data Protection Impact Assessment (DPIA) for the activity.

The ROPA is held on SharePoint head office, reviewed annually by the Director and on every material change (new system, new processor, new processing activity, new home, new category of children). The Information Asset Register at the home (held by the RM) is the per-home view that feeds the ROPA.

20. International Transfers

Personal data is transferred outside the UK only where the relevant safeguards under UK GDPR Chapter V are in place — an adequacy regulation, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU SCCs, or another approved transfer mechanism. Where ICG's processors host data outside the UK or process it elsewhere, the relevant transfer mechanism is in the Data Processing Agreement.

21. Vendor and Processor Management

- Every processor handling ICG personal data is subject to a written Data Processing Agreement that satisfies Article 28 UK GDPR.
- The DPA is signed by the Director and by the processor before any personal data is shared.
- The DPA sets out: the subject-matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subjects; the obligations and rights of the controller; the processor's obligations including security, sub-processors, data subject rights, breach notification, audit, deletion or return on termination.
- Sub-processors require the Director's prior written authorisation; the processor remains fully liable to ICG for the sub-processor's performance.
- Annual processor review — the Director reviews each processor against contractual commitments and against any breach or incident in the year.

22. Training and Awareness

Training	Audience	Frequency	Provider
Induction data protection briefing — covering this policy, the role of the DPO, lawful basis, data subject rights, breach reporting, the seven golden rules	Every employee before any unsupervised shift	Once at induction	HR Manager / Director
Annual data protection refresher	Every employee	Annual	HR Manager / Director
Information sharing — Working Together + seven golden rules	Every member of staff working with children	Induction + annual	Internal led by RM
SAR handling	RM, Deputy Manager, HR Manager, Director	On appointment + 2-yearly refresher	External / Director
DPIA and ROPA	Director, Information Asset Owners	On appointment + 2-yearly refresher	External
Personal Data Breach response	Every member of staff (awareness) + DPO and Information Asset Owners (in depth)	Induction + annual + tabletop exercise	Internal led by Director

Training	Audience	Frequency	Provider
		yearly	

23. Audit and Assurance

- Monthly — Information Asset Owners confirm in the Manager Monthly Audit on Nourish that JML actions for their system are complete and access lists are current.
- Monthly — DPO reviews the SAR Register and the Breach Register; flags any pattern or unresolved item to the Director.
- Quarterly — the Director reviews the ROPA against actual processing, samples access logs across systems, and signs the quarterly information governance summary.
- Twice-yearly — the RI samples information governance as part of the Reg 45 audit (sample SARs, sample sharing decisions, sample access logs, ROPA spot-check).
- Annually — the Director re-signs the ROPA; every Information Asset Owner runs full access recertification (Section 16.4); processors reviewed against DPAs (Section 21); ICO Accountability Framework self-assessment completed and any actions captured.
- Ad hoc — on any actual breach, on any near miss above threshold, on any change in legislation or ICO guidance, on any new system or processor.

24. Related Policies

Policy	Why it links
Records Management Policy + Records Retention Schedule	How long records are kept, where they are stored, when and how they are destroyed; the retention schedule sits as Appendix to that policy.
IT and Cybersecurity Policy	Technical security measures, acceptable use, device management, IT asset register.
Safeguarding and Child Protection Policy	Information sharing in safeguarding contexts; LADO routing; Working Together.
Reporting Notifications Policy	Reg 40 routing for any safeguarding-engaged breach.
Safer Recruitment and Onboarding Policy	DBS, references, pre-employment checks — processing lawful basis and special-category conditions.
Grievance and Disciplinary Policy	Just Culture / Decision Matrix routing for any staff data-protection breach.
Finance Recording and Reporting Policy	Special-category data in young-person spending records; data retention for HMRC and Children's Records.
Use of Personal Mobile Devices Policy + Social Media Policy	Personal device boundaries; staff online conduct.
Artificial Intelligence Policy	Emma AI processing of child data; human-in-the-loop principles aligned to Article 22.
CCTV and Surveillance (where engaged) — DPIA required before deployment	Surveillance-specific lawful basis and proportionality.

Policy	Why it links
Confidentiality undertakings for visitors and contractors	Standard form for any third party with incidental access to personal data.
Health and Safety Policy	Health data of staff (sickness, occupational health) — special-category condition.
Business Continuity and Critical Incident Policy	Article 6(1)(d) vital interests engaged in critical incidents.

25. Review Log

Version / reason	Date	Reviewed by
v1.0 — Initial issue.	24/05/2026	Dr Shaurya Maheshwari (Director and DPO)

Appendix A — Lawful Basis Reference Card

Laminated for staff offices and held on Sona. Use this card to confirm the lawful basis for any new processing activity before it starts.

Article 6 — General lawful basis

Basis	When to use at ICG
(a) Consent	Used only where the data subject genuinely has a free choice — e.g. photo / video / personal anecdote for marketing.
(b) Contract	Employment contract; offer of placement where the Company is contracted with the placing authority.
(c) Legal obligation	CHR 2015, HMRC, RIDDOR, Reg 40, statutory employment law obligations.
(d) Vital interests	Critical incidents where life is at risk.
(e) Public interest task	ICG is not a public authority; engaged where ICG is supporting the placing authority's s.22 / s.11 duty.
(f) Legitimate interests	Internal management reporting; documented Legitimate Interests Assessment required.

Article 9 — Special-category conditions (most common at ICG)

Condition	When to use at ICG
(2)(b) Employment / social security / social protection	Employee health records; sickness; occupational health.
(2)(c) Vital interests where incapable of consent	Medical emergency for a placed child or staff member.
(2)(g) Substantial public interest + DPA 2018 Sch 1 para 18 safeguarding	Safeguarding of placed children; safeguarding of vulnerable people in the home; the primary basis for child special-category data.
(2)(h) Provision of health or social care	Health data processed to deliver the care; needs DPA 2018 Sch 1 para 2 safeguards.
(2)(f) Legal claims	Where engaged in actual or anticipated proceedings.

Appendix B — Subject Access Request Form

A SAR may be made by any means, including verbally — this form is provided for convenience and is not required. Submitted to dpo@insightcare.uk or by post to the home or to head office, addressed to the Data Protection Officer.

Field	Your entry
Full name	
Date of birth (where relevant — e.g. former placed child)	
Current address and contact details	
Email address for response (preferred)	
Relationship to ICG (current employee / former employee / placed child / former placed child / parent or guardian with parental responsibility / other)	
Authority to act on behalf of the data subject (where you are not the data subject — provide evidence)	
Period covered by the request (where you can narrow it)	
Specific data you are asking for (where you can narrow it — e.g. "my Sona record"; "my Nourish entries from January to March 2026"; "all my data"). The Company will tell you what it holds at a system level if you do not yet know what to ask for.	
Format preferred (electronic by default; paper available)	
Identity verification provided	(e.g. driving licence + utility bill; Sona login for current employee; placing-authority letter for placed-child SAR by third party)
Date of request	
Signature	

Appendix C — Subject Access Request Workflow

The DPO holds a master copy. Used by RM and HR Manager when a SAR arrives at the home or HR. Detailed in Section 14.

Step	Owner	Deadline
1. SAR received	RM (home request) / HR Manager (employee request)	Day 0
2. Acknowledge to requester; forward to DPO	RM or HR Manager	Within 5 working days
3. Verify identity	DPO	Day 5 - 10
4. Apply MCA / Gillick competence (child SAR)	DPO with RM input	Day 5 - 10
5. Scope and search	DPO with Information Asset Owners	Day 10 - 20
6. Redact and apply exemptions	DPO	Day 20 - 25
7. Compile response and send securely	DPO	Within one month of verified ID
8. Log on SAR Register and close	DPO	Same day as response
9. Quarterly audit	Director	Quarterly
Extension (up to + 2 months for complex / numerous)	DPO with Director approval	Notify requester within first month

Appendix D — RBAC Access Matrix Template

One sheet per system. Held on SharePoint by the Information Asset Owner. Updated on every JML event and at the annual recertification.

Field	Content
System name	(Sona / Nourish / Eploy / Camascope / Emma AI / SharePoint home / SharePoint head office / M365 tenant / Revolut Business / Payroll / external accountant)
Information Asset Owner	
DPA in place — yes/no, date signed, next review	
User list — name, role, home, access level, date provisioned, last activity, next recertification	
Privileged access — admin and super-user accounts, who holds them, MFA enforced	
Recent changes (since last review) — joiners, movers, leavers, ad-hoc access	
Anomalies — any access that does not fit the typical pattern, with the reason	
Sign-off — Information Asset Owner name, date; Director annual sign-off	

Appendix E — Data Protection Impact Assessment (DPIA) Template Headings

Completed before any new high-risk processing starts. Signed by the Director. Held on SharePoint head office.

Section	Content
Header	Project / processing name; Information Asset Owner; date drafted; Director sign-off date; next review.
Step 1 — Identify the need for a DPIA	What the project is, what it involves, why a DPIA is needed (any of the Article 35 triggers — large-scale special category, systematic monitoring, new technology, etc.).
Step 2 — Describe the processing	Nature, scope, context and purposes. What data is processed, how, who has access, how long, how it is shared, where it is held.
Step 3 — Consultation	Who has been consulted internally and externally (data subjects, RI, DPO, ICO where engaged).
Step 4 — Necessity and proportionality	Lawful basis, special-category condition, purpose limitation, data minimisation, retention.
Step 5 — Identify and assess risks	For each risk: source, likelihood, severity, overall.
Step 6 — Identify measures to reduce risk	For each risk: control measure, effect on risk (eliminated / reduced / accepted), residual risk.
Step 7 — Sign-off	DPO advice; Information Asset Owner agreement; Director sign-off; ICO consultation under Article 36 where any residual high risk cannot be mitigated.
Step 8 — Review	Review at least every 2 years and on any material change.

Appendix F — Personal Data Breach Notification Template

Used to record every breach and near miss. Drives the Article 33 ICO notification and the Article 34 data subject notification where the thresholds are met.

Field	Content
Breach reference (Sona auto)	
Date and time of breach (where known)	
Date and time detected	
Detector — name, role	
Type — confidentiality / integrity / availability — or combination	
Description — what happened, what was the data, who is affected (categories of data subjects and approximate numbers)	
Containment action taken — what was done in the first minutes / hour / day	
Cause — root cause and contributing factors	
Risk assessment — likelihood of harm to data subjects, severity, overall risk	
ICO notification — Y / N / not yet decided; reference number where notified	
Data subject notification — Y / N / not yet decided; how and when	
Other notifications — LADO / placing authority / Reg 40 / police	
Investigation outcome — what we learned, what we changed	
Remediation actions with named owner and date	
Director sign-off and date	
RI quarterly audit reference	

Appendix G — Information Sharing Decision Card

Laminated for staff offices. Use before sharing any confidential information about a child, an employee or another data subject with anyone outside ICG.

Stop

- Is this a routine share covered by the Placement Plan, an existing court order, or the worker's contract? If yes, share and record.
- If not — go through the seven golden rules below.

Seven Golden Rules

- 1. The Data Protection Act 2018 / UK GDPR does not prevent the sharing of information for the purposes of safeguarding children — it provides a framework for doing so.
- 2. Be open and honest with the child / family / worker about why, what, how and with whom — unless doing so would put a child at risk of harm.
- 3. Seek advice from the RM, the DPO or the Caldicott Guardian if in doubt.
- 4. Share with consent where appropriate; respect the wishes of those who do not consent — unless there is a justified reason to share without consent.
- 5. Necessary, proportionate, relevant, adequate, accurate, timely and secure.
- 6. Keep a record of every decision to share AND of every decision NOT to share — with the reason.
- 7. Share by the right route — never personal email; never personal WhatsApp; secure channel only.

Caldicott check

- Justify the purpose. Use minimum information. Strict need-to-know. The duty to share is as important as the duty to protect.

Appendix H — Retention Schedule Cross-Reference

The detailed retention schedule sits in the Records Management Policy (Appendix A of that policy). The principal retention periods that this policy refers to:

Category	Retention	Source
Child case file (placed children)	75 years from date of birth	IRMS toolkit; CHR 2015 Reg 36
Employee record (after end of employment)	6 years from end of employment; longer for any RIDDOR-linked record (40 years)	Limitation Act 1980; RIDDOR
Payroll / tax record	6 years from end of tax year	HMRC
Finance record (Revolut, weekly upload, Manager Monthly Audit financial tab)	6 years from end of tax year	HMRC
SAR record	3 years from completion of SAR	ICO best practice
Personal data breach record	3 years from breach close; longer if the breach engages a child record or HR case file	ICO best practice
DPIA record	Life of the processing + 6 years	ICO best practice
ROPA	Live; superseded versions retained 6 years	ICO best practice
CCTV / body-worn footage	Per the relevant DPIA (typically 30 days unless engaged in an incident)	Per DPIA
Visitor sign-in book	6 years	Fire and safeguarding records