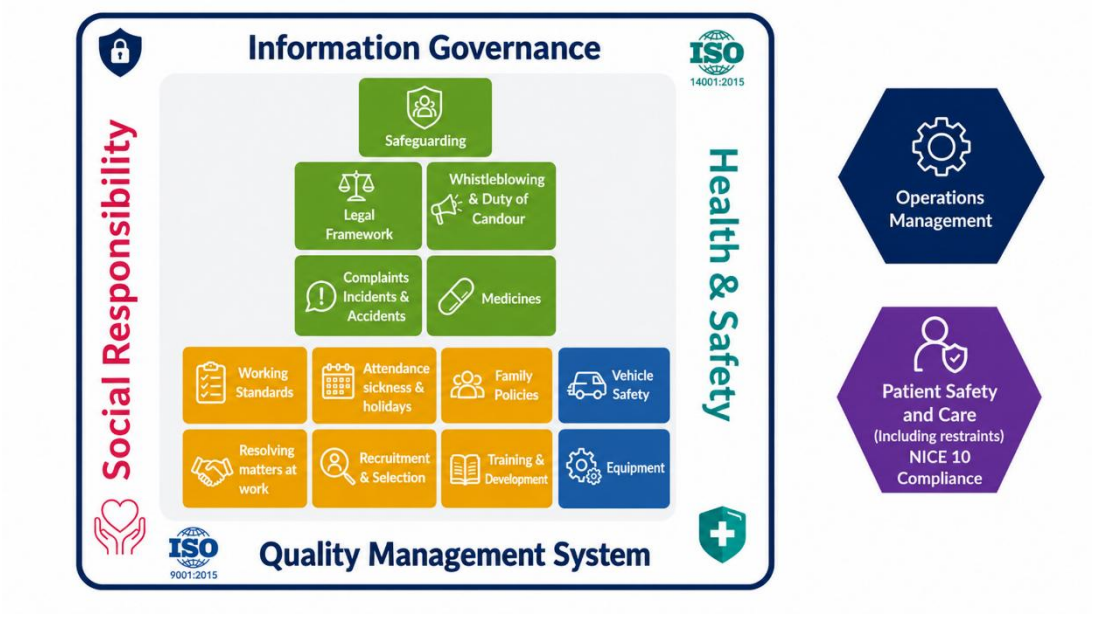
Secure Care UK Policy Framework

Policy Title:

Information Governance.v6.0

SECURECARE UK

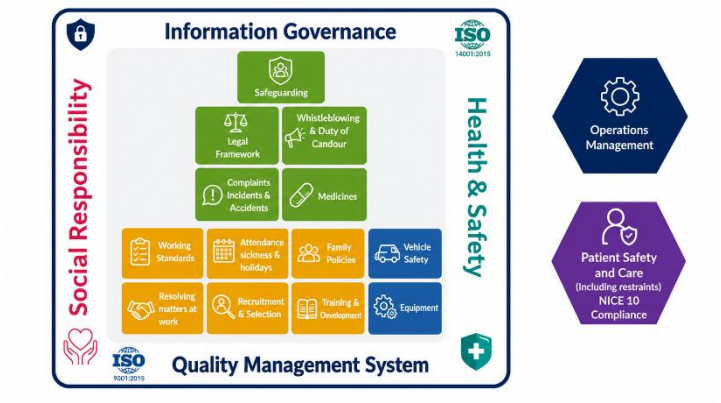


Approved: Paul Denne Finance and IT Manager (Data Protection & SIRO)	Last Reviewed Date: 01/07/2026
Approved: Matt Jackson Managing Director (Caldicott Guardian)	Last Reviewed Date: 02/07/2026

The Secure Care Policy Framework.

Secure Care UK has a clear policy structure which is managed using our ISO 9001 quality framework. We are keen to ensure that we have a clear and easily understood basis to our policies and where individual topics require documentation and policy consideration, we will attempt to add these sections into our current framework to avoid increasing our number of policies. The benefit of this approach is that we can ensure that the risk of contradictions and confusion is reduced, and we are able to insist that policies are understood by our team. All policies are freely available to all team members on our internal communication IT platform and on a designated SharePoint.

Our policies fall into 4 broad categories as shown in the diagram below.



Overarching Policies

We have four overarching policies which we see as the crucial “bedrock” of what we do, these are the Information Governance Policy which includes compliance with NHS Data Protection and Anti-Fraud requirements, Our Health and Safety Policy (H&S), our Governance and Quality (ISO 9001) Framework and our Social Responsibility Policy which includes Environmental considerations. These four overarching policies are shown in the large square as they surround and control all other policies.

People, Resources and Clinical Policies

We have three groups of important, detailed policies covering the three topic areas above. These three policy categories are strongly influenced by our Overarching Policies above (IG, H&S, GRF, SR) which are all considered in detail in the writing and ongoing development of all People, Resource and Clinical Policies. Our Clinical Policies layout how we embrace the rules and guidelines required by our regulating bodies. Our People Policies are consolidated into our Employee Handbook.

Standard Operating Procedure Policies

Our final two policies describe how we practically deliver our service to our patients and clients these are our Operations Management and Patient Safety and Care Policies. These describe

the practical application of our care on a day-to-day basis. These policies incorporate our ISO 9001 Process which are our 14 Standard Operating Procedures

Document Control

Date	Version	Comments
22.12.2020	V2.0	Policy Framework added
12/06/2025	V5.0	Update version number in line with new system
12/08/2025	V5.1	Updated administration fee for SAR
17/10/2025	V5.2	Updated for Cyber Essential needs, password control
01/07/26	V6.0	Updated references and CCTV

Review Control

Reviewer	Section	Comments	Date
Paul Denne	All	Currently under review	22.12.20
Paul Denne	All	Reviewed V3	17.08.21
Paul Denne	All	Reviewed V4	17/08/22
Paul Denne	All	Reviewed V5	07/09/23
Matt Jackson	All	Reviewed V5 – no changes	15/09/23
Paul Denne	All	Reviewed amend 14.2 now V6	07/09/23
Paul Denne	All	Reviewed V6.1	15/09/24
James Harry	N/A	Version changed to v5.0 in line with new numbering system	12/06/2025
Paul Denne	All	Reviewed V6.0	01/07/2026

Table of Contents

1. Purpose

This policy has been prepared and published in recognition of Secure Care UK's obligations under UK data protection legislation. Secure Care UK processes personal information in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable legislation and regulatory guidance. The organisation is committed to ensuring that personal information is processed lawfully, fairly, transparently and securely.

We believe that to the best of our ability the approaches outlined within this policy enable our full compliance with our obligations. The purpose of the policy is to establish general standards for Information Governance including all aspects of data protection and information systems management and to distribute responsibility for their achievement to all managers, supervisors, and other employees through the normal line management processes.

2. Scope

a. The scope of this policy will cover all of the business activities undertaken by Secure Care UK including the management of supplier and sub-contracting relationships. This policy applies to all employees within the organisation and also identifies where particular responsibilities are assigned to members of the management structure.

   This policy, together with the associated standards, applies to the management of all documents and records, in all technical or physical formats or media, created or received by Secure Care in the conduct of its business activities. It applies to all staff, contractors, consultants and third parties who are given access to our documents and records and information processing facilities. It is intended to describe how Secure Care UK discharges its obligations under relevant UK legislation and regulatory requirements, including but not limited to:

   • UK General Data Protection Regulation (UK GDPR)
   • Data Protection Act 2018
   • Data (Use and Access) Act 2025
   • Freedom of Information Act 2000
   • Privacy and Electronic Communications Regulations (PECR), where applicable
   • Computer Misuse Act 1990
   • Health and Social Care (Safety and Quality) Act 2015
   • NHS Data Security and Protection Toolkit requirements (where applicable).

b. The nature of the activity undertaken by Secure Care UK necessitates the use of CCTV for the protection of our colleagues and patients. This policy will include within its scope the management of the images and recordings from any CCTV systems.
c. The table below provides a listing of the tangible and intangible assets impacted by this policy.

Personal Information Content	Software
• Databases and data files • Back-up and archive data • Audit data • Paper records (patient case notes and staff records) • Paper reports	• Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware including PCs, Laptops, PDA, communications devices eg. blackberry and removable media
System/Process Documentation	**Miscellaneous**
• System information and documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services eg. power and air-conditioning • People skills and experience • Shared service including Networks and Printers • Computer rooms and equipment • Records libraries

3. Responsibilities

- It is the responsibility of the Managing Director to review this document and to recommend its approval to the board. As Secure Care UK is a relatively small organisation the Managing Director will undertake the duties of Caldicott Guardian supported by our main board's Clinical Advisor.
- Our Head of Finance and IT will be accountable for the implementation of this policy and will act as the Serious Information Risk Owner (SIRO) and the Data Protection Officer
- The Quality Manager will monitor the delivery of all audits described within this policy and ensure that the Governance Committee and board review all audits and instruct the management team to take actions as a result of these audits.
- It is the responsibility of all employee with any management responsibilities to ensure that the requirements of this policy are communicated, trained and where necessary, enforced.
- It is the responsibility of all employees at Secure Care to follow this policy and these obligations will be made clear in all contracts of employment.

4. Definitions

- SOP's – Standard Operating Procedures
- SIRO – Senior Information Risk Owner

5. Related Documents

- Employee Handbook
- SOPs
- Register of systems
- Business Continuity Plan
- Data Protection Impact Assessment Tool (Appendix 1)
- Transparency Statement (Appendix 2)
- Staff Information Security Guidance

6. Policy Audit

Secure Care UK (Secure Care) fully accepts the obligations placed upon it by the various Acts of Parliament and its contracts and responsibilities. A programme of audits will be undertaken to ensure we robustly test our systems and processes. These audits will include (but are not limited to):

• A Data Quality Audit • An archiving compliance audit • A review of the register of systems • An annual audit of staff training along with a survey of staff opinions on data security in line with the latest questions in the NHS Data Protection and Security Toolkit recommendations • Results and actions from the annual penetration test if appropirate	• A Data Protection Impact Assessment Compliance Audit • Annual Systems Stress Test including a review of anti-virus and security outputs • The quality of information in the annual submission of the NHS Data Protection and Security Toolkit • Audit of data disposals contractor

7. Data protection principles

Secure Care UK is committed to processing personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025. The organisation will ensure that all processing activities comply with the data protection principles set out within Article 5 of the UK GDPR together with any subsequent amendments introduced through UK legislation. Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
g. When Secure Care UK enters into a substantial new client relationship or implements a new system the Head of Finance and IT acting as the Data Protection Officer and SIRO shall conduct and act upon a Data Protection Impact Assessment (Appendix 1)
h. The organisation will follow NHS guidance and undertake Cyber essentials accreditation

Legislative Monitoring

The Head of Finance and IT, acting as the Data Protection Officer and Senior Information Risk Owner (SIRO), shall monitor changes to UK data protection legislation, Information Commissioner's Office (ICO) guidance and NHS Data Security and Protection Toolkit requirements. Where legislative or regulatory changes affect Secure Care UK's processing activities, this policy, associated procedures and staff guidance shall be reviewed and updated accordingly.

General provisions

a. This policy applies to all personal data processed by the organisation.
b. The Head of Finance and IT shall take responsibility for the organisation's ongoing compliance with this policy as the organisations nominated Data Protection Officer.
c. Secure Care UK shall register with the Information Commissioner's Office as an organisation that processes personal data. Our registration number is ZA243852

Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the organisation shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner and as per the commitments made in the organisations Data Transparency Statement (See Appendix 2). This statement will be available via our website.

Lawful purposes

a. All data processed by the organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Organisation shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in Secure Care's systems.

Data minimisation

a. Secure Care shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. The Organisation will adopt the principle of pseudonymisation when dealing with personal data and will ordinarily utilise the initials of an individual e.g. John Smith would become "JS".

Accuracy

a. The organisation shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. To ensure that personal data is kept for no longer than necessary, the organisation shall put in place an archiving standard for each area in which personal data is processed and review this process annually.
d. The archiving standard shall consider what data should/must be retained, for how long, and why and is shown below:

Data Type	Retention Period	Exceptions	Exceptions to be agreed by
Booking forms and patient risk assessments.	6 months	Any open investigations	Quality Manager
Records of employees who have left the organisation	6 years HMRC	Open legal cases	Managing Director
Invoices, remittance advices and expense claims	6 years HMRC	Open legal cases	Head of Finance and IT
Patient Care Records	7years	Any Open investigations	Quality Manager
Patient opinion surveys	1 year		Quality Manager
CCTV	30 days	Any Open investigations	Regional Manager
Vehicle and asset check document	7 years		Head of Finance and IT

e. The Head of Finance and IT will ensure that destruction certificates are obtained and recorded for all hard copy document confidential data destruction

Security, Passwords, Systems & CCTV/Body Cams

a. The organisation shall ensure that personal data is stored securely using modern software that is kept-up to date.
b. All users shall maintain a secure minimum 12 digit password (no maximum) for login into computer systems and software that is unique to them, not shared and does not use common phrases or names. The use of at least three random words is recommended.
c. In the event of any password being lost or suspected to be compromised it must be reported immediately to Head of IT and Orbital 10 to be recorded, reset and assessed for Data Breaches.
d. All Tablets and devices will use a min 6 digit pin code where required.
e. Request for new users must be sent to Head of IT with details of access level required and business needs case for access. New Administrator accounts must also be requested to Head of IT, with full details of scope of access and period of access required which then must be approved by the Board.
f. Leavers will be notified by HR and users removed from systems by HR and Head of IT.
g. The organisation shall ensure that anti-virus and general security protections are deployed and updated automatically on a weekly basis.
h. Administration accounts will only be used for the specific installation of programs and updates as needed. To obtain any downloads required a Standard user account must be used and all access to internet and email must only be via a standard user account. The use of an administrator account to browse the internet or access email is strictly forbidden
i. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
j. When personal data is deleted this should be done safely such that the data is irrecoverable.
k. Appropriate back-up and disaster recovery solutions shall be in place.
l. An annual stress test of systems shall be undertaken
m. The Head of Finance and IT will maintain a register of all systems and include within this any areas where the latest releases of software are not in use and any High-Risk data. These results will be reviewed as a standing item at our monthly governance meeting and issues escalated to the Board.
n. All members of staff shall be trained to at least level 1 data security with an annual refresher to be recorded through the eLearning portal.
o. The organisation will follow NHS guidance and undertake annual Cyber Essentials certification

CCTV Governance

Secure Care UK uses Closed-Circuit Television (CCTV) systems within selected offices, operational hubs and other company premises to support the safety and security of our colleagues, patients, visitors and company property. CCTV is operated in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the principles contained within this Information Governance Policy.

Purpose of CCTV

The purposes of CCTV are to:

- Protect colleagues, patients, contractors and visitors.
- Deter, prevent and detect criminal activity including theft, vandalism and unauthorised access.
- Assist with the investigation of reported incidents including security breaches, accidents, complaints, allegations of bullying or harassment and other serious workplace concerns.
- Protect company assets and premises.
- Support investigations where footage may be required as evidence for disciplinary, grievance, insurance or legal proceedings.

CCTV will not be used for the routine monitoring of employees or for assessing employee performance. Footage will only be viewed where there is a legitimate operational reason or where an incident has been reported.

Lawful Basis

Secure Care UK processes CCTV images under Article 6(1)(f) of the UK GDPR (Legitimate Interests).

The organisation has a legitimate interest in maintaining the safety and security of its employees, patients, visitors, premises and property. The use of CCTV has been assessed as necessary and proportionate to achieve these purposes while minimising any impact on the privacy of individuals.

Where CCTV or body-worn camera footage contains special category personal data, including information relating to an individual's health or care needs, Secure Care UK will additionally rely upon Article 9(2)(h) UK GDPR (management of health and social care services) and, where relevant, Article 9(2)(f) UK GDPR (the establishment, exercise or defence of legal claims).

A Data Protection Impact Assessment (DPIA) shall be completed before installing any new CCTV system, repositioning an existing camera, materially changing a camera's field of view, introducing body-worn cameras, or where there is any significant change to monitoring arrangements or the purpose of processing.

Camera Positioning

Cameras shall be positioned only where necessary to achieve the stated security purposes.

Cameras may monitor communal areas such as:

- Reception areas
- Building entrances and exits
- Corridors
- Waiting areas

- Car parks
- External access points

Camera positioning will be carefully assessed to minimise the collection of unnecessary personal data and to avoid excessive surveillance.

Cameras shall be configured to minimise recording beyond Secure Care UK's premises wherever reasonably practicable.

Private Areas

CCTV cameras will not intentionally monitor or record areas where individuals have a reasonable expectation of privacy.

This includes, but is not limited to:

- Toilets
- Changing facilities
- Shower rooms
- Staff rest facilities where privacy would reasonably be expected
- Private offices unless justified by an identified security risk

Where cameras are positioned near these areas, they will be adjusted to ensure they do not capture unnecessary footage.

Signage

Clear and prominent CCTV signage shall be displayed at the entrance to all monitored premises and within monitored areas where appropriate.

The signage will inform individuals that CCTV is in operation, identify Secure Care UK as the data controller and provide contact details for further information regarding the processing of personal data.

Access to CCTV Footage

Access to recorded CCTV footage is strictly controlled.

Routine viewing of CCTV footage to monitor employees is prohibited.

Footage may only be accessed where there is a legitimate operational need, including:

- Investigation of reported incidents
- Allegations of bullying, harassment or misconduct

- Security incidents
- Theft, criminal damage or unauthorised access
- Health and Safety investigations
- Insurance or legal proceedings

Access is restricted to:

- The Data Protection Officer (SIRO)
- Regional Managers

Where appropriate, access may be authorised for the Managing Director or any investigator appointed by the organisation.

All access to CCTV footage shall be recorded within an access log detailing the reason for viewing, the individual accessing the footage and the date of access.

Disclosure of CCTV Footage

CCTV recordings will only be disclosed where there is a lawful basis to do so.

Footage may be disclosed to:

- Police and law enforcement agencies investigating criminal offences.
- Courts or other bodies where disclosure is required by law.
- Insurers or legal advisers in connection with claims or legal proceedings.
- Other organisations where there is a lawful obligation or lawful basis for disclosure.

Any disclosure shall be documented and approved by the Data Protection Officer or an authorised senior manager.

Subject Access Requests

Individuals have the right to request access to CCTV images of themselves under the UK GDPR.

Requests will be managed through Secure Care UK's Subject Access Request process.

Where footage includes images of other identifiable individuals, Secure Care UK will consider whether the footage can be provided through redaction or whether an exemption applies under the Data Protection Act 2018.

Requests relating to CCTV footage should be submitted as soon as reasonably practicable to maximise the likelihood that footage remains available within the retention period.

Retention of CCTV Footage

CCTV recordings shall be retained in accordance with the organisation's Records Management Schedule (Section 7.5). The standard retention period is 30 days unless required for an ongoing investigation, legal proceedings, insurance claim or police enquiry.

Footage required for an ongoing investigation, disciplinary process, grievance, insurance claim, police investigation or legal proceedings may be retained for longer where necessary. Any such extension must be authorised by the Regional Manager. Once the matter has concluded, the footage will be securely deleted in accordance with the organisation's Records Management Schedule.

Annual Review

The necessity and effectiveness of each CCTV installation shall be reviewed at least annually.

The review will consider:

- Whether CCTV remains necessary.
- Whether the lawful basis remains appropriate.
- Whether camera locations remain proportionate.
- Whether any privacy risks have changed.
- Whether retention periods remain appropriate.
- Whether signage remains accurate and visible.

Where CCTV is no longer justified, the system or individual cameras will be removed or repositioned.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) shall be completed before:

- Installing any new CCTV system.
- Introducing additional cameras.
- Significantly changing camera coverage or purpose.
- Introducing new recording technologies or monitoring arrangements.

The DPIA will assess the necessity, proportionality and privacy risks associated with the proposed processing and identify any measures required to reduce risks to individuals before the system becomes operational.

Breach

a. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the organisation shall

promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

b. The Head of Finance and IT in the role as SIRO will maintain a record of any data protection breaches and report these immediately to the Quality Manager who will arrange a formal investigation and inform the Managing Director of progress.

8. Information Security Principles

a. This section outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Secure Care UK information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 7 Caldicott principles compliance with the NHS Information Governance Toolkit.

Caldicott
1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

b. The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.
For Secure Care UK the core principles are impacted, and the effect aggregated, when any data breach relates to patient care data.

c. Governance – Roles and Responsibilities

a. All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Secure Care UK's business. All staff are responsible for information security and remain accountable for their actions in relation to Secure Care and other UK Government information and information systems. Staff **shall** ensure that they understand

their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

b. Head of Finance and IT

The Head of Finance and IT shall act as the Senior Information Risk Owner (SIRO) and is accountable for information risk within Secure Care and advises the Board on the effectiveness of information risk management across the organisation. The Head of Finance and IT will also undertake the role of Data Protection Officer and is responsible for ensuring implementation of this policy Data Security Standards with respect to Patient Confidential Data. (S)he

- Communicate and promote awareness of the Act across Secure Care
- Lead on matters concerning individuals right to access information held Secure Care and the transparency agenda.
- Monitor developments in UK data protection legislation, including the Data (Use and Access) Act 2025, and ensure organisational policies and procedures remain compliant.

c. Support from Clinical Advisor

It is recognised that the services provided by Secure Care UK are clinical in nature and that the advice of a qualified and registered clinician is important particularly when advising the Managing Director in his/her role as Caldicott Guardian. The Chairman of the board will make arrangements to ensure that the board has a suitably qualified clinician as an advisor.

d. Senior Responsible Owners

All Senior Managers, Heads of Department, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that this policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:

- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within the business area(s) for Information Security
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

e. On a regular basis and as a minimum as part of an annual review the top 3 Information Governance risks will be noted on the company risk register and reviewed in detail by the board.

Compliance Requirements

Audit

Audit will be performed as part of the ongoing Secure Care Audit Programme and the Information Security Officer shall ensure appropriate evidence and records are provided to support these

activities at least on an annual basis. The Quality Manager is accountable to the Governance Committee and the board to ensure this programme is undertaken

Review

This policy shall be reviewed at least annually by the reviewers noted within the Reviewers section of this policy. The Head of Finance and IT shall be responsible for ensuring the review is conducted in good order and follows due process for approval.
The Head of Finance and IT is accountable for providing the results of ongoing reviews of information security implementation across Secure Care. This includes support to the annual NHS Data Security and Protection Toolkit delivery.
On an annual basis the organisation will conduct the NHS DSP survey of colleagues.

Records Management

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management protects the interests of Secure Care UK, its employees, patients, commissioners and everyone who interacts with the organisation. Records, and the information they preserve, are important organisational assets.
We aim to balance our commitment to openness and transparency with our responsibility for patient and employee confidentiality. So, we will create and manage records efficiently, make them accessible where possible, protect and store them securely and dispose of them safely at the right time.
By adopting this policy, we aim to ensure that the record, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to:

- help us carry out our business
- help us to make informed decisions;
- protect the rights of employees,
- regulated entities, and the public;
- track policy changes and development;
- make sure we comply with relevant legislation;
- provide an audit trail to meet business, regulatory and legal requirements;
- make sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence;
- support continuity and consistency in management and administration
- make sure we are open, transparent and responsive
- support research and development
- promote our achievements.

The organisation will maintain a register of systems which will include within it if there is any personal data captured and stored within the system. This format is shown in appendix 3. The register of systems will be audited annually and the results reported to the Governance Committee and the Board of Directors.

9. Freedom of information Act

9.1 The Freedom of Information Act 2000 (the Act) provides a right of public access to information held by organisations providing services to public bodies. Secure Care UK is committed to its obligations under the Act which require it to do the following:

- Publish certain information about its activities
- Respond to requests for information

9.2 Under the terms of the Act individuals may submit written requests for information to the organisation and these will be accepted via email as described in our Data Transparency Statement

9.3 Requestors have a right to be informed within 20 working days whether the organisation holds the requested information and if so, subject to paragraph 8.4 to receive a copy of the information.

9.4 There are 23 exemptions under the Act which entitle Secure Care UK to withhold information if it considers it is appropriate to do so. If the decision is made to withhold the information it will provide the requestor with the following:

- Confirmation, if appropriate, whether the requested information is held
- Details of the appropriate exemption under the Act
- Reasons why it considers the exemption applies
- Details of the review procedure.

9.5 Information which can be complied accurately within 2-3 hours will normally be provided free of charge.

9.6 Secure Care UK complies with the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations (2004). All requests that take less than 2-3 hours or £100 (being the "appropriate limit") to process will be free of charge. If the estimated time for compliance is in excess of 3 hours then the organisation may refuse the request or alternatively may issue an invoice for the estimated cost, such invoice to be paid before the organisation undertakes its retrieval of the requested information.

10. Internal Review and Complaints

10.1 Requestors have the right to ask for an internal review of how their request has been handled. This includes where the requested information has been withheld.

10.2 Such requests should be submitted in writing to info@securecareuk.co.uk

10.3 The internal review will be carried out by the Managing Director within 20 working days of receipt.

10.4 If the requestor is dissatisfied with the outcome of the internal review then they can appeal the decision to the Information Commissioner's Office (ICO) which oversees compliance with the Act. The ICO can be contacted at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF.
Telephone 0303 1231113.
Email: casework@ico.org.uk

11. Clarity of Employee Obligations

11.1. All employees will be required to undertake Data Protection e learning within their first week within Secure Care UK.

11.2. All employment contracts will include the following clauses:

- You shall comply with all relevant data protection legislation and/or any Secure Care UK policy regarding data protection when processing personal data in the course of employment including personal data relating to any employee, patient or agent of Secure Care UK.
- In order to manage your contract of employment and for related purposes, such as updating and enhancing our records, analysis for management purposes and statutory returns, legal and regulatory compliance and crime prevention, you have supplied us with your personal data and we can therefore process, use and disclose personal data about you as is necessary in compliance with data protection legislation. Some data may be supplied to external suppliers who administer employee benefits, solely for the purpose of providing those benefits to you.
- Secure Care UK may make such information available to those who provide products or services to the Secure Care UK (such as advisers and payroll administrators), regulatory authorities, potential or future employers, governmental or quasi-governmental organisations.
- Secure Care UK expects you to inform your line manager of changes to your personal data in a timely manner

12. Policy Revision

This policy statement will be reviewed on an annual basis and as required to ensure continue compliance with legislative requirements and to take account of any changes in Secure Care UK operational arrangements.

An earlier review will be undertaken where there are significant changes to UK legislation, Information Commissioner's Office guidance, NHS Data Security and Protection Toolkit requirements or organisational processing activities.

13. Assessment of impact on other policies

Health and safety	Limited
Governance and Reporting	High
Vehicle Safety	Medium
Equipment	Medium
Diversity and Inclusions	Limited
Employee Conduct	Medium
Recruitment and Induction	Medium
Skills, capability and training	High
MCA, MHA, NICE	Medium
Whistleblowing and Duty of Candour	High
Complaints, Incidents and Accidents	High
Medicines	Limited

Operations Management	High
Patient Safety and Care (including restraints)	High

14. Policy Implementation

14.1. Meetings/Governance Bodies tasked with responsibilities by this policy

The board of Directors has a responsibility to review Information Governance Matters at each Board Meeting.
The Governance Board is responsible for a detailed review of all Information Governance Matters and to ensure that the annual audit

14.2. Measurement and monitoring requirements as a result of this policy.

Annual Audits as per section 6.1
E learning Compliance
NHS Data Security and Protection Toolkit delivery and annual refresh
Annual Colleague Data protection survey
POWER BI Data review

14.3. Standard Operating Procedures Impacted by this policy

To be updated as SOP are re-written

14.4. Training impacts of this policy

All employee UK GDPR training
SIRO and Caldicott Guardian training

14.5. Roles within this organisation tasked with responsibilities

Managing Director
Head of Finance and IT
Quality Manager
Training Manager
All members of the Leadership Team

14.6. Other implementation considerations

A review of all hub locations to ensure there are appropriate storage of patient care records and booking forms

14.7. How will we know that this policy is working?

Annual audit
Opportunities for proactive improvements are being identified routinely at Governance Board Meetings

The annual team survey will show improvement in the “Safe place to work” categories
The results of the annual survey on data protection as recommended in the NHS Data Security and Protection Toolkit.

15. Appendix 1 – Data Protection Impact Assessment Screening Checklist

Data Protection Impact Assessment Screening Checklist	SECURE CARE UK SECURE PATIENT TRANSPORT SPECIALISTS

New Process or Relationship:

Overview:

Should a Data Protection Impact Assessment be Carried out?

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ evaluation or scoring;

☐ automated decision-making with significant effects;

☐ systematic monitoring;

☐ processing of sensitive data or data of a highly personal nature;

☐ processing on a large scale;

☐ processing of data concerning vulnerable data subjects;

☐ innovative technological or organisational solutions;

☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;

☐ process special-category data or criminal-offence data on a large scale;

☐ systematically monitor a publicly accessible place on a large scale;

☐ use innovative technology in combination with any of the criteria in the European guidelines;

☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare or match data from multiple sources;

☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ process personal data that could result in a risk of physical harm in the event of a security breach.

☐ Installation of CCTV or other surveillance technology

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

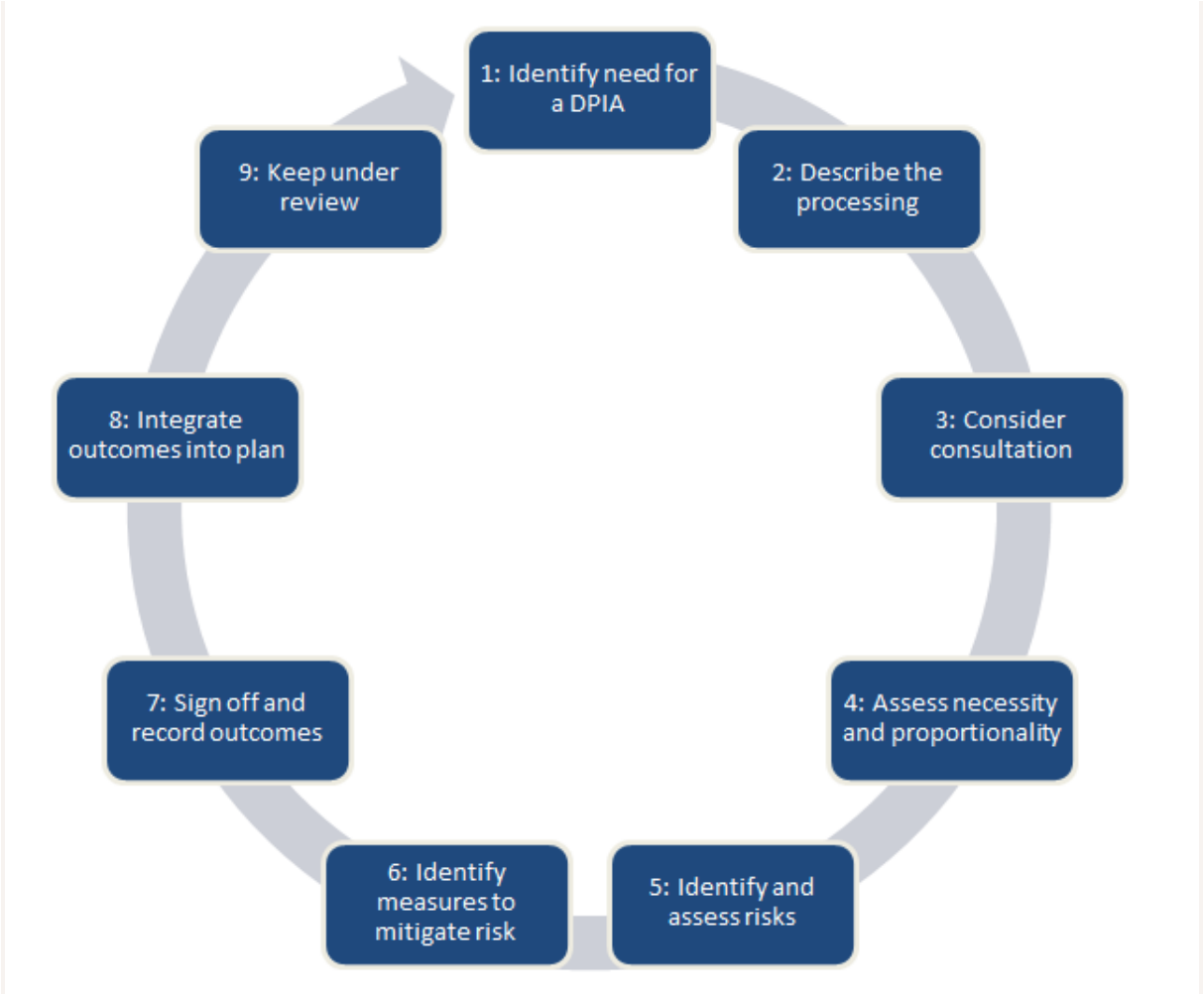
☐ If we decide not to carry out a DPIA, we document our reasons.

Should a Data Protection Impact Analysis be conducted? Yes or No (please circle)

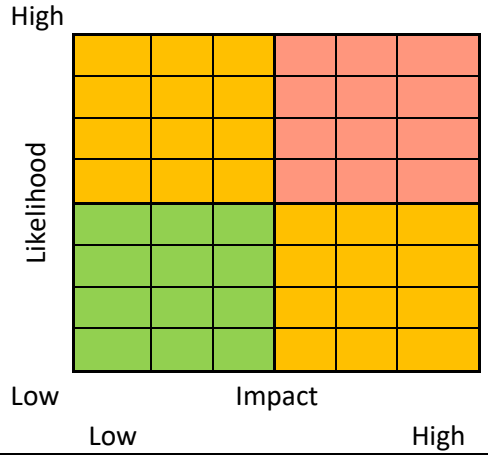
Reason for decision:

If Yes continue below. In No

Data Protection Impact Analysis Steps



Describe the data processing which will occur
Is there a need to consult with clients or patient groups? Considering necessity and proportionality
What are the risks and what would be the impact/likelihood of any issues?
Please place a “X” in one square. (One table for each risk)



What Contingencies and Mitigations are to be implemented as a result of this assessment?

No	Action	Who	By when or complete

Formally accepted by Governance Committee on:

Formally accepted by Board on:

Full Implementation check diarised for:

Full Implementation signed off by……. On ……

16. Appendix 2– Data Transparency Statement

Your rights

Data protection laws in the UK give people a number of rights concerning their personal data. Not all rights apply equally to all our processing activity as certain rights are not available depending on the lawful basis for the processing. These rights are:

1. Right to be informed
2. Right of access
3. Right to rectification
4. Right to erasure
5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Rights in relation to automated decision making and profiling.

We want you to feel confident that we look after everyone's personal data in line with the law. If you have any questions about your rights, you can get in touch with us at info@securecareuk.co.uk

Requesting a copy of your information

Typically, we collect information from health and care organisations providing your care and would advise contacting them directly for a more complete record of your care or treatment. We do not hold your whole medical or care record.

If you would like to request a copy of your personal data that Secure Care UK is processing, then you will need to complete a subject access request. Please email info@securecareuk.co.uk and place "Subject Access Request" in the title of the email.

Following your request, we may contact you within the statutory response period to clarify or narrow the scope of your request where appropriate. Where requests are particularly complex or numerous, Secure Care UK may extend the response period by up to a further two months in accordance with the UK GDPR. You will be informed if an extension is required and the reasons for it. Individuals have the right to access their personal data and any such requests made to the organisation shall be dealt with in a timely manner and as per the commitments made in the organisations Data Transparency Statement (See Appendix 2). This statement will be available via our website. In accordance with the UK GDPR, the Data Protection Act 2018 and the Data (Use and

Access) Act 2025. Secure Care UK will not normally charge a fee for responding to Subject Access Requests. However, in accordance with the UK GDPR and the Data Protection Act 2018, the organisation reserves the right to charge a reasonable administrative fee where requests are manifestly unfounded, excessive or for additional copies of the same information. This fee reflects both internal administrative time and any external costs incurred in locating, retrieving, reviewing, and reproducing the data.

Sharing information

There are very strict rules about who can access the personal data we process, and what it can be used for. When information is shared with other organisations, these organisations have to go through an audit and have a clear data management agreement in place with ourselves.

Where necessary Secure Care UK will undertake a Data Protection Impact Assessment prior to the commencement of any new major system project or any substantial new business relationship or contract. Copies of Data Protection Impact Assessments can be requested by way of an email to info@securecareuk.co.uk

CCTV Processing

Secure Care UK operates CCTV systems at selected premises for the purposes of protecting employees, patients, visitors, contractors, company property and investigating reported incidents. CCTV is operated under Article 6(1)(f) UK GDPR (Legitimate Interests).

Images are normally retained for 30 days and may be disclosed to law enforcement agencies or other authorised bodies where there is a lawful basis to do so. CCTV is not used for routine employee monitoring.

Data retention

All data is retained and erased in accordance with our Record Management Schedule. Specific retention periods are identified within each processing purpose listed below. If a specific purpose requires a different retention period outside of our policy this will be explained.

Complaints

If you wish to raise a complaint concerning Secure Care UK's processing activity please do so via our website. You also have the right to raise a concern with the Information commissioner's Office at any time.

17. Appendix 3– Format of Register of Systems

Register of systems and personal data

Last updated 11/07/2019

Location	Data Processor	Owner	Volume	Personal data and legal basis	Access	Shared/Published	Format	Retention	Risks / impact	Key asset