THE ORCHARD PARTNERSHIP

Old Orchard Surgery | Spring Orchard Surgery | Till Orchard Surgery | Cherry Orchard Surgery

Information Governance, Data Protection and Confidentiality Policy

Applies to all four sites of The Orchard Partnership | Version 1.0 | May 2026

Document Control

Policy Title	Information Governance, Data Protection and Confidentiality Policy
Version	1.0
Date Issued	May 2026
Review Date	May 2027 (or earlier if legislation changes)
Author	Head of Communications and Sustainability, The Orchard Partnership
Approved By	Practice Manager, The Orchard Partnership
Applies To	All staff, contractors, volunteers and third parties working at or on behalf of any of the four sites of The Orchard Partnership
Sites	Old Orchard Surgery (Wilton), Fovant Surgery, Shrewton Surgery, Codford Surgery
ICB	NHS Bath and North East Somerset, Swindon and Wiltshire Integrated Care Board (BSW ICB)
Supersedes	N/A — new additional policy
Status	Active

1. Purpose

The Orchard Partnership (TOP) is committed to handling all personal, confidential and sensitive information in a lawful, ethical, secure and transparent manner. This policy sets out the framework within which the partnership manages information governance (IG) across all four of its GP surgery sites in Wiltshire.

The purpose of this policy is to:

- Set out the legal and regulatory framework within which TOP processes personal and confidential information
- Establish the roles and responsibilities of all staff, contractors and third parties who handle personal data on behalf of TOP
- Define how patient confidentiality is protected, and the limited circumstances in which information may be shared or disclosed without consent
- Ensure TOP meets its obligations under the NHS Data Security and Protection Toolkit (DSPT) and all applicable legislation
- Protect TOP from legal liability, reputational harm and regulatory action arising from information governance failures
- Support a culture of information governance awareness and accountability across all four sites

This policy should be read alongside all related policies in TOP's information governance suite, including its Privacy Notices, Data Breach Procedure, Subject Access Request Procedure and any site-specific confidentiality agreements.

2. Scope

This policy applies to:

- All permanent and temporary members of staff employed by The Orchard Partnership, at any of its four sites
- Locum clinicians, bank staff, trainees, student placements and volunteers
- Contractors, cleaning staff, IT providers, and any other third parties who may have access to, or come into contact with, personal identifiable information held by TOP while on any of the practice premises
- Any processing of personal data carried out on behalf of TOP by a third-party data processor, where TOP acts as the data controller

The policy covers personal data in all formats — electronic, paper, audio, visual, and information held in memory.

3. Legislative and Regulatory Framework

The Orchard Partnership operates within a complex legislative and regulatory environment. This policy has been developed to ensure compliance with all of the following:

3.1 Primary Legislation

- UK General Data Protection Regulation (UK GDPR) — the principal data protection law governing the processing of personal data
- Data Protection Act 2018 (DPA 2018) — complements UK GDPR, provides exemptions and sets out the role of the Information Commissioner's Office (ICO)
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, Regulation 17 — CQC fundamental standard on good governance
- Common Law Duty of Confidentiality — an established legal obligation to preserve the confidentiality of information provided in confidence
- Freedom of Information Act 2000 — governs public access to information held by public authorities, including access to deceased patients' medical records (s.41)
- Access to Health Records Act 1990 — governs access to medical records of deceased patients by certain applicants
- Human Rights Act 1998, Article 8 — right to respect for private and family life
- Mental Capacity Act 2005 and its Code of Practice — governs decision-making for individuals lacking capacity
- Medical Act 1983 — duties of registered medical practitioners
- Gender Recognition Act 2004 — imposes specific statutory restrictions on disclosure of protected information
- Computer Misuse Act 1990 — criminalises unauthorised access to computer systems

3.2 NHS Frameworks and Guidance

- NHS Records Management Code of Practice 2021 (updated) — mandatory records retention and disposal framework for NHS organisations in England
- NHS Data Security and Protection Toolkit (DSPT) — mandatory annual self-assessment tool measuring compliance with national data security standards
- National Data Guardian's Data Security Standards — ten standards drawn from the 2016 Caldicott review (National Data Guardian for Health and Social Care)
- The Eight Caldicott Principles (including the eighth principle added in 2020: Inform patients and service users about how their confidential information is used)
- NHS England Information Governance Policy (updated May 2025)
- GMC Guidance: Confidentiality — good practice in handling patient information (2024)
- BMA Confidentiality and Health Records Toolkit (2025)
- NHS Code of Practice on Confidential Information

> ⚠ **Important:**
> Where any conflict appears to exist between this policy and the legislative requirements set out above, the legislative requirements will take precedence. This policy will be updated promptly whenever relevant legislation or NHS guidance changes.

4. The Eight Caldicott Principles

The Caldicott Principles are at the heart of The Orchard Partnership's approach to information governance. They apply to all uses of confidential patient information, both within and between organisations. The eighth principle, added in 2020, strengthens the requirement for transparency with patients about how their information is used.

No.	Principle	Application at The Orchard Partnership
1	**Justify the purpose for using confidential information**	We will document the purpose for any use or disclosure of patient identifiable information before it takes place.
2	**Use confidential information only when necessary**	We will always consider whether anonymised data could serve the same purpose before using identifiable information.
3	**Use the minimum necessary confidential information**	Access to and use of information is limited to the minimum required to achieve the stated purpose.
4	**Access on a strict need-to-know basis**	Role-based access controls are applied to all clinical systems. Staff access only the information required for their specific role.
5	**All staff must understand their responsibilities**	All staff receive mandatory annual information governance training and sign a confidentiality agreement on appointment.
6	**Comply with the law**	All processing of personal data complies with UK GDPR, the Data Protection Act 2018, and applicable NHS guidance.
7	**The duty to share is as important as the duty to protect**	We recognise that failure to share information can be as harmful as inappropriate disclosure. We support lawful information sharing for patient care.
8	**Inform patients about how their information is used**	We maintain up-to-date privacy notices across all four sites and proactively inform patients about data use.

5. UK GDPR Data Protection Principles

The Orchard Partnership, as a data controller, must process all personal data in accordance with the six data protection principles set out in Article 5 of UK GDPR. All staff processing personal data on behalf of TOP must adhere to these principles at all times:

1. Lawfulness, fairness and transparency	Personal data must be processed lawfully, fairly and in a transparent manner. Patients must be informed about how their data is used via up-to-date privacy notices at all four sites.
2. Purpose limitation	Data collected for a specified purpose must not be used for any other purpose that is incompatible with the original purpose, unless the patient has given consent or there is a lawful basis to do so.
3. Data minimisation	Only data that is adequate, relevant and limited to what is necessary for the stated purpose may be collected and processed.
4. Accuracy	Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be corrected or erased without delay.
5. Storage limitation	Personal data must not be held for longer than is necessary. TOP follows the NHS Records Management Code of Practice 2021 for minimum retention periods.

6. Integrity and confidentiality (security)	Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

In addition to these six principles, UK GDPR introduces a seventh overarching principle: Accountability. TOP must not only comply with the data protection principles but must be able to demonstrate that compliance. This policy, alongside the practices' DSPT submission, privacy notices, staff training records and data processing agreements, forms part of that evidence of accountability.

6. The Duty of Confidentiality

6.1 Scope of the Duty

The duty of confidentiality applies to all personal identifiable information held by The Orchard Partnership, including information held in electronic and paper records, visual and audio recordings, and information known from memory or direct patient contact. The duty extends to:

- All clinical information, diagnoses, treatment records and prescriptions
- Demographic information including names, addresses, dates of birth and NHS numbers
- Information about appointments, test results, referrals and hospital attendances
- Any other information that could, alone or in combination, identify an individual patient
- Staff personal data, employment information and HR records

The duty of confidentiality is not limited to clinical staff. It applies to every member of TOP's team — clinical, administrative, managerial and operational — and extends beyond employment to cover the period following termination of employment.

6.2 Confidentiality Agreements

All staff will be required to sign a confidentiality agreement as part of their employment contract or on commencement of their role with TOP. Contractors, IT providers, cleaners and any third parties who may have incidental access to personal identifiable information while on any of the practice premises must also sign a confidentiality agreement before commencing work.

6.3 Private Spaces

All conversations, telephone calls, and clinical discussions involving patient information must take place in private spaces — consulting rooms, offices, or enclosed meeting areas — away from areas accessible to other patients or the general public. Reception staff must take particular care when handling patient queries at the desk and must use the private consultation area available at each site for sensitive discussions.

7. Consent, Lawful Basis and Information Sharing

7.1 Lawful Basis for Processing

UK GDPR requires that all processing of personal data has a lawful basis. For health data — which is classified as a special category under UK GDPR — the lawful basis most relevant to TOP's work is:

- Article 6(1)(e) — processing necessary for the performance of a task carried out in the public interest, and Article 9(2)(h) — processing necessary for the provision of health or social care treatment
- Article 6(1)(a) and Article 9(2)(a) — explicit consent of the data subject, where required
- Article 6(1)(c) — processing necessary for compliance with a legal obligation

TOP will document the lawful basis for processing in its records of processing activities (ROPA) and in its privacy notices. Staff must never process patient data without being satisfied that a lawful basis exists.

7.2 Implied and Explicit Consent

Patients are generally considered to have given their implied consent for relevant information about them to be shared among the clinical team involved in their care, on a need-to-know basis. This implied consent does not extend to sharing information with third parties, family members, or for non-clinical purposes.

Explicit consent — where the patient actively agrees, verbally or in writing — is required for disclosures that fall outside direct clinical care, including but not limited to: insurance reports, employer reports, legal proceedings where the patient is the applicant, research involving identifiable data, and sharing with social services outside an urgent safeguarding context.

7.3 Sharing with Other Health Professionals

Information sharing between health professionals involved in a patient's direct care is both lawful and necessary. TOP staff share information relevant to patient care on a strictly need-to-know basis. The seventh Caldicott Principle reflects this: the duty to share information for individual care is as important as the duty to protect it.

When sharing information with social services, community teams or integrated care teams, patients must normally give their explicit consent unless the disclosure is required by law, there is an overriding public interest, or there is a safeguarding concern.

7.4 When Disclosure is Permitted Without Consent

There are limited circumstances in which information may be disclosed without a patient's consent. These include:

- When required by law — health professionals are obliged to report certain conditions and incidents regardless of patient consent
- When there is an overriding public interest — serious and imminent threat to public health, national security, life of an individual, prevention or detection of serious crime
- Safeguarding — where there are concerns about abuse or neglect of a child or vulnerable adult
- Disclosure to courts, tribunals or regulatory bodies exercising their legal powers

In all cases where information is disclosed without consent, the minimum necessary information must be shared, the disclosure must be documented with clear justification, and the Caldicott Guardian should be consulted where there is any doubt.

7.5 Anonymisation and Pseudonymisation

Wherever possible, data used for purposes other than direct patient care — such as audit, commissioning, research or quality improvement — should be anonymised or pseudonymised. Pseudonymised data remains personal data and must be treated accordingly. Fully anonymised data, from which no individual can reasonably be identified, is not subject to UK GDPR but staff should seek advice from the practice's Data Protection Officer before treating data as anonymised.

8. Specific Categories of Patient

8.1 Children and Young People

People under the age of 16 in England are presumed not to have capacity to consent to the disclosure of their own health information, unless individually assessed as Gillick competent — that is, demonstrating sufficient understanding and intelligence to make their own informed decisions. TOP staff must apply Gillick competency and Fraser guidelines as appropriate and seek senior clinical guidance in cases of uncertainty.

Where a child is Gillick competent, they are entitled to the same duty of confidentiality as an adult, including the right to request that their information is not shared with their parents.

8.2 Adults Who Lack Mental Capacity

The Mental Capacity Act 2005 presumes that all adults aged 16 and over have capacity to make decisions about their own information unless assessed otherwise. Capacity is decision-specific and time-specific.

Where a patient lacks capacity to consent to disclosure, information may be shared with relatives, carers or representatives only to the extent necessary to assess and serve the patient's best interests. Best interests decisions must be objective, documented, and must take into account the patient's previously expressed wishes and feelings, their beliefs and values, and the views of those close to them.

Where no next of kin, Lasting Power of Attorney or Court of Protection deputy is available, an Independent Mental Capacity Advocate (IMCA) should be consulted for decisions about serious medical treatment.

8.3 Deceased Patients

The duty of confidentiality continues after a patient's death. Medical records of deceased patients remain confidential, subject to specific rights of access under the Access to Health Records Act 1990. Personal representatives and individuals with a potential claim arising from the death may have a right of access to relevant information, subject to the practice's discretion.

The last registered GP practice is responsible for handling Access to Health Record (AHR) requests for deceased individuals. Primary Care Support England (PCSE) administers requests where the last registered practice is closed.

9. Operational Data Security

9.1 Electronic Records

All staff with access to clinical systems must:

- Use individual login credentials — Smartcards or passwords must never be shared
- Log out of all computer systems whenever leaving a workstation unattended
- Clear the screen of any patient record before accessing another patient's information
- Change passwords at regular intervals and immediately upon any suspected breach
- Never attempt to access records for which they have no clinical or administrative need
- Report any suspicious access attempts or system anomalies to the practice's IT lead without delay

9.2 Paper and Manual Records

Paper records and other physical documents containing personal data must be:

- Held in secure, locked storage at all times when not in active use
- Never left unattended or visible to unauthorised persons
- Tracked when removed from filing for clinical or administrative purposes, and returned promptly
- Kept on site unless there is a specific, documented reason for temporary removal
- Disposed of securely using cross-cut shredding or approved confidential waste services

9.3 Email and Electronic Communication

Personal identifiable information must only be transmitted electronically using secure methods. Specifically:

- All patient identifiable data sent externally must be transmitted via an NHS.net email account or another NHS-approved encrypted channel
- Wherever possible, clinical details and demographic data should be separated in electronic communications
- Fax machines must not be used for the transmission of patient identifiable or confidential clinical information
- Personal data must not be sent via personal (non-NHS) email accounts under any circumstances
- Staff working remotely must use only NHS-approved or practice-approved secure systems to access patient data, in line with the practice's home working procedure

9.4 Mobile Devices and Portable Media

Personal data must not be stored on portable devices such as USB drives, personal mobile phones or laptops unless these are encrypted and have received prior approval from the practice IT lead and ICB team. Lost or stolen devices containing personal data must be reported immediately as a potential data breach.

9.5 CCTV

Where present, CCTV is installed at TOP's surgery sites for the prevention and detection of crime and for the safety of staff and patients. The use of CCTV complies with the ICO's CCTV Code of Practice. Notices are displayed at all sites where CCTV is in operation. CCTV footage will only be disclosed where there is a lawful basis, such as to the police with public interest justification. Footage is retained in line with the practice's retention schedule.

9.6 Call Recording

Patient telephone calls may be recorded at TOP's surgery sites for the purposes of training, quality assurance and the resolution of disputes. Patients are always informed that calls may be recorded before a call commences. All recordings form part of the patient's clinical record and are subject to the same duty of confidentiality as all other patient information. Recordings may be accessed under a Subject Access Request.

10. Data Breach Management

10.1 Definition

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches may be deliberate (e.g. unauthorised access by a member of staff) or accidental (e.g. a misdirected email or lost paper record).

10.2 Reporting

All actual or suspected data breaches — however minor — must be reported immediately to the Senior Information Risk Owner (SIRO) and the practice's Data Protection Officer (DPO). Staff must never attempt to conceal or resolve a data breach independently.

Statutory reporting timescale:

Under UK GDPR Article 33, the Information Commissioner's Office (ICO) must be notified of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals within 72 hours of TOP becoming aware of it.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, the affected individuals must also be notified without undue delay (UK GDPR Article 34).

Not all breaches require reporting to the ICO — the DPO will assess the severity and likelihood of risk and determine whether reporting is required. All breaches, however minor, must be recorded in TOP's internal breach log regardless of whether external reporting is required.

Serious data security incidents must also be reported through the NHS Data Security and Protection Toolkit (DSPT) incident reporting mechanism. The DSPT automatically refers high-severity incidents to the ICO.

10.3 Investigation and Learning

All reported breaches will be investigated by the SIRO and DPO. The investigation will seek to establish: what happened, what personal data was involved, the likely impact on affected individuals, and what steps can be taken to prevent recurrence. Findings and any resulting changes to practice will be documented.

11. Records Management and Retention

The Orchard Partnership follows the NHS Records Management Code of Practice 2021 (as updated) for all records retention and disposal. Key principles are:

- Patient clinical records must remain with the practice until the patient registers elsewhere, dies, or is otherwise deregistered, after which they are formally transferred via Primary Care Support England (PCSE)
- The electronic patient record will be automatically or manually extracted when the patient registers elsewhere or is notified as deceased
- Non-clinical records (staff, employment, administrative) will be retained for the minimum periods set out in the NHS Records Management Code of Practice and disposed of securely thereafter
- Any decision to extend a retention period beyond the minimum specified must be documented with clear justification
- Records relating to any ongoing or anticipated legal proceedings, inquiries or regulatory investigations must not be destroyed until the relevant authority confirms it is safe to do so

A separate records retention schedule is maintained by the practice and is available to all staff. Staff must not destroy any records without following the approved disposal procedure and must use a confidential waste service or cross-cut shredding for paper documents.

12. Subject Access Requests

Under UK GDPR, individuals have the right to access personal data held about them by submitting a Subject Access Request (SAR). Patients, staff and other individuals may exercise this right in relation to data held by The Orchard Partnership.

Patients wishing to access their medical records should submit a written request to their surgery. A SAR response must be provided within one calendar month of receipt of the request. This period may be extended by a further two months in cases of complexity or volume, provided the individual is informed of the extension within the initial one-month period.

SARs are usually provided free of charge. A reasonable fee may be charged where requests are manifestly unfounded or excessive. The practice will only charge in exceptional circumstances and with clear documented justification.

All SARs are handled in accordance with TOP's Subject Access Request Procedure and by the designated lead at each site.

13. Specific Disclosure Scenarios

13.1 Disclosure to the Police, Social Services and Partner Organisations

Some statutes permit, rather than require, disclosure of patient information to the police, social services or partner organisations. In such cases, information may only be shared where the patient has given consent, where there is an overriding public interest, or where there is a safeguarding concern. The minimum necessary information must always be shared, and the disclosure must be documented and justifiable.

13.2 Safeguarding

Where TOP has concerns about the safety of a child or vulnerable adult — including where there are concerns about abuse or neglect — the duty to protect overrides the duty of confidentiality. Information must be reported promptly to the appropriate statutory body. Concerns and actions taken must be clearly documented in the patient record. Staff should refer to TOP's Safeguarding Policy for further guidance.

13.3 Legal Proceedings and Solicitors

Health records required for legal proceedings are usually obtained via the Data Protection Act 2018 or the Access to Health Records Act 1990. Written consent from the patient is required before releasing records to a solicitor acting on behalf of the patient. Where there is any doubt about the extent of information to be disclosed, legal advice must be sought.

13.4 Disclosure to Courts and Regulatory Bodies

Courts, coroners' courts, certain tribunals and regulatory bodies including the General Medical Council have legal powers to require disclosure of information relevant to matters within their jurisdiction, without the patient's consent. TOP will comply with lawful orders to disclose information while limiting disclosure to the minimum required.

13.5 Complaints

Where a patient makes a formal complaint, investigation of that complaint will require access to relevant parts of their health record. Patients must be made aware of this. Only information directly relevant to the complaint will be used. Where a third party (such as an MP) is involved in the complaint process with the patient's written consent, only relevant information may be shared with them. A copy of any response must be sent to the patient.

13.6 Serious Communicable Diseases

Information about serious communicable diseases remains particularly sensitive. The practice will follow GMC guidance and relevant legislation when considering any disclosure, including in relation to contact tracing. Every effort will be made to obtain the patient's voluntary consent before any disclosure. Where a patient refuses and there is a genuine risk to a third party, the practice will seek legal and ethical guidance before proceeding.

13.7 Media and Press

The Orchard Partnership will not disclose identifiable patient information to the press or media without the patient's explicit written consent. Any media enquiry relating to patient care must be referred immediately to the Senior GP Partner and the Head of Communications and Sustainability. Where a patient or family member has used the press to raise concerns, TOP may respond only to the extent of noting that information used appears to be inaccurate or incomplete, without disclosing any confidential details.

14. Roles and Responsibilities

14.1 Caldicott Guardian

The Caldicott Guardian is a senior clinician at The Orchard Partnership with overall responsibility for protecting the confidentiality of patient information and enabling appropriate and lawful information sharing. The Caldicott Guardian:

- Ensures TOP meets the highest practical standards for handling patient identifiable information
- Oversees and advises on all decisions relating to information sharing and disclosure
- Ensures that confidentiality considerations are reflected in TOP's policies, procedures and strategic decisions
- Acts as the champion for information governance and confidentiality across all four sites

14.2 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is a senior partner or registered provider at The Orchard Partnership responsible for:

- Taking overall ownership of TOP's information risk strategy
- Understanding and managing how information risks could impact the delivery of services
- Leading the information governance risk assessment and management processes
- Taking accountability for risk-based decisions relating to the processing of personal data
- Ensuring TOP's DSPT submission is completed and submitted annually

14.3 Data Protection Officer (DPO)

The Orchard Partnership has appointed a Data Protection Officer (DPO) in line with UK GDPR Article 37, provided by the ICB. The DPO operates independently and reports to the SIRO. The DPO's responsibilities include:

- Advising TOP and its staff on compliance with data protection legislation
- Monitoring compliance with UK GDPR and TOP's internal data protection policies
- Being the first point of contact for the ICO
- Advising on Data Protection Impact Assessments (DPIAs) for new or changed data processing activities
- Managing the data breach reporting process
- Providing guidance on Subject Access Requests

14.4 Communications Manager

The Head of Communications and Sustainability at TOP has operational responsibility for:

- Maintaining and updating this policy and all related information governance documentation
- Co-ordinating the annual DSPT submission in conjunction with the SIRO and DPO
- Ensuring privacy notices across all four sites are accurate, up to date and accessible to patients
- Overseeing staff information governance training records and ensuring compliance with mandatory annual training
- Managing data breach reporting and maintaining the breach log
- Acting as the point of contact for information governance queries from staff

14.5 All Staff

Every member of TOP's team is personally responsible for:

- Reading, understanding and complying with this policy and all associated information governance procedures

- Completing mandatory annual information governance training via the NHS Data Security Awareness training module or equivalent
- Reporting any actual or suspected data breach or information security concern immediately
- Never accessing, using or disclosing personal data except in the performance of their legitimate duties
- Seeking guidance from the Caldicott Guardian or DPO when uncertain about a disclosure decision

14.6 Third Parties and Contractors

Third parties accessing any TOP site — including IT providers, maintenance contractors, external consultants and cleaning staff — must sign a confidentiality agreement before commencing work. Data processing agreements must be in place with all third parties who process personal data on behalf of TOP, in accordance with UK GDPR Article 28.

15. Training and Awareness

All staff at The Orchard Partnership must complete mandatory information governance training on an annual basis. This training covers: data protection and UK GDPR, confidentiality, information security, data breaches, and the Caldicott Principles. Completion of training is monitored by the Communications Manager.

New starters must complete information governance training within their first four weeks in post and before being granted unsupervised access to any clinical system or patient records.

Training records are maintained by the practice and form part of TOP's DSPT evidence.

16. NHS Data Security and Protection Toolkit (DSPT)

Completion of the NHS DSPT is a mandatory requirement for all GP practices in England. The Orchard Partnership is required to submit its annual DSPT self-assessment, demonstrating compliance with the National Data Guardian's ten data security standards. The SIRO has overall responsibility for the DSPT submission, supported by the Communications Manager.

The DSPT encompasses: information governance policies, staff training, data security, data breach management, third-party assurance, business continuity planning, and data flows. Non-compliance with the DSPT may affect TOP's ability to access NHS systems and could result in regulatory action.

17. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a legal requirement under UK GDPR Article 35 where proposed data processing is likely to result in a high risk to the rights and freedoms of individuals. DPIAs must be completed before introducing:

- New clinical or administrative systems involving the processing of patient data
- Any significant change to existing data processing activities
- New data sharing arrangements with third parties or partner organisations
- Any processing involving large-scale use of special category (health) data

The DPO must be consulted in the preparation of all DPIAs. Completed DPIAs are retained as evidence of TOP's accountability obligations.

18. Patient Rights Under UK GDPR

Patients whose personal data is processed by The Orchard Partnership have the following rights under UK GDPR, which TOP will honour:

Right to be informed	Patients are entitled to clear information about how their data is used, provided via privacy notices at each site and on the practice websites.
Right of access	Patients may request access to their personal data via a Subject Access Request (see Section 12).

Right to rectification	Patients may request that inaccurate or incomplete data is corrected.
Right to erasure	In limited circumstances, patients may request deletion of their data. This right does not override the legal requirement to retain clinical records for the minimum periods set out in the NHS Records Management Code.
Right to restrict processing	Patients may request that processing of their data is restricted in certain circumstances.
Right to data portability	Patients may request their data in a structured, machine-readable format where applicable.
Right to object	Patients may object to certain types of processing, including use of data for research or direct care planning without their consent.
Right not to be subject to automated decisions	TOP does not use automated decision-making or profiling that produces legal or similarly significant effects on patients.

Any exercise of these rights should be referred to the DPO or designated lead at the relevant site. Requests will be dealt with within the statutory timeframe of one calendar month.

19. Monitoring and Review

This policy will be reviewed annually, by no later than May 2027, or earlier in the event of:

- A change in relevant legislation, UK GDPR guidance or NHS contractual requirements
- A significant data breach or information governance incident
- Findings from the annual DSPT submission that require a policy update
- A CQC inspection identifying gaps in information governance

Compliance with this policy is monitored through: annual DSPT submission, staff training records, data breach logs, SAR response records, and clinical governance meetings. A summary of information governance compliance will be included in the annual governance report presented to the GP Partners.

20. Key Definitions

Caldicott Guardian	A senior person within a health or social care organisation with responsibility for protecting the confidentiality of patient information and enabling lawful and appropriate information sharing.
Data Controller	An organisation that determines the purposes and means of processing personal data. The Orchard Partnership is the data controller for all patient and staff data it processes.
Data Processor	An organisation that processes data on behalf of a data controller, under a written data processing agreement. Examples include cloud system providers and external IT support.
Data Protection Officer (DPO)	A designated individual with specialist knowledge of data protection law, responsible for monitoring compliance, advising on DPIAs and liaising with the ICO.
DSPT	The NHS Data Security and Protection Toolkit — a mandatory annual self-assessment tool measuring compliance with NHS data security standards.
Information Governance (IG)	A framework for handling personal information in a confidential, secure and appropriate manner, covering legal compliance, confidentiality, data security and records management.
Personal Data	Any information relating to an identified or identifiable living individual, including names, NHS numbers, addresses, dates of birth and clinical information.
ROPA	Record of Processing Activities — a documented log of all personal data processing activities carried out by TOP, required under UK GDPR Article 30.
SIRO	Senior Information Risk Owner — a senior member of the organisation with overall accountability for information risk management.

Special Category Data	Data that requires extra protection under UK GDPR Article 9, including health data, genetic data, racial or ethnic origin, religious beliefs, sexual orientation and trade union membership.
Subject Access Request (SAR)	A formal request by an individual to access the personal data held about them by an organisation. Must be responded to within one calendar month under UK GDPR.
UK GDPR	The UK General Data Protection Regulation — the primary data protection legislation in force in the United Kingdom following the UK's exit from the European Union.

21. Related Policies and Documents

This policy forms part of The Orchard Partnership's information governance suite, which may also include:

- Privacy Notices — General Patient Privacy Notice; Children's Privacy Notice; Staff Privacy Notice; Software-specific privacy notices
- Data Breach Reporting Procedure
- Subject Access Request Procedure
- Confidentiality and Complaints Policy
- Records Management and Retention Schedule
- Home Working Policy
- Data Processing Agreements with third-party processors
- DSPT Annual Submission Evidence Pack