BloodWorks Ltd

Policy Suite

Information Governance

Suite content

Approval Date	29.07.26
Review Date	29.07.27
Review Frequency	Annual
Applies To	All employees, directors, self-employed practitioners, associate clinicians, volunteers, students, contractors, agency workers and anyone representing BloodWorks
Status	Live

BloodWorks Ltd

Information Governance and Confidentiality Policy

Document Information

Policy Title	**Information Governance and Confidentiality Policy**
Policy Category	Governance
Policy Owner	Data Protection Lead / Registered Manager
Approved By	Director and Senior Responsible Officer
Version	2.0
Approval Date	30.07.26
Review Date	30.07.27
Review Frequency	Annual
Applies To	All employees, directors, self-employed practitioners, prescribers, associate clinicians, subcontractors, volunteers, contractors, agency workers and anyone representing BloodWorks
Status	Draft

Information Governance at a Glance

Our Commitment

Confidentiality – Respect • Trust • Privacy

Information Security – Accuracy • Security • Accountability

Good Governance – Lawfulness • Transparency • Continuous Improvement

Always

✓ Collect only the information necessary for the service being provided.

✓ Keep personal and confidential information secure.

✓ Share information only where there is a lawful basis.

✓ Respect every person's right to privacy and confidentiality.

✓ Record information accurately and professionally.

✓ Report suspected information security incidents immediately.

Never

✗ Access information without a legitimate work-related reason.

✗ Discuss confidential information where others may overhear.

✗ Share information without appropriate authority or lawful justification.

✗ Store confidential information on unauthorised devices or systems.

✗ Leave confidential information unsecured.

✗ Ignore actual or suspected data breaches.

If you're unsure...

Data Protection Lead / Registered Manager

↓

Director / Senior Responsible Officer

1. Statement of Intent

BloodWorks Ltd recognises that the safe, lawful and ethical management of information is fundamental to delivering high-quality healthcare and maintaining the confidence of the people and communities we serve.

Every person accessing a BloodWorks service has the right to expect that their personal information will be treated with dignity, respect and confidentiality. This applies equally whether services are delivered from a clinic, community health hub, outreach venue, workplace, mobile clinic or through digital consultation. Information governance is therefore embedded throughout every aspect of BloodWorks' clinical and organisational practice.

BloodWorks processes personal and special category information in order to deliver preventative healthcare, diagnostic and screening services, clinical assessment, prescribing, ongoing monitoring, health optimisation and harm reduction interventions. The organisation also works collaboratively with laboratories, pharmacies, NHS organisations and other partner agencies where appropriate to support safe, integrated and person-centred care.

Many people who engage with BloodWorks have experienced barriers to accessing mainstream healthcare, including individuals affected by health inequalities, recovery communities, criminal justice populations, people using image and performance enhancing drugs (IPEDs), and other marginalised groups. The organisation recognises that maintaining confidentiality and handling information sensitively are essential to building trust and encouraging continued engagement with healthcare services. Confidentiality is therefore viewed not simply as a legal obligation but as a cornerstone of compassionate, person-centred practice.

BloodWorks is committed to ensuring that personal information is:

- Collected fairly, lawfully and transparently.
- Limited to what is necessary for the service being provided.
- Accurate, relevant and kept up to date.
- Stored securely using appropriate technical and organisational safeguards.
- Accessible only to those with a legitimate need to know.
- Shared only where there is a lawful basis or with the individual's consent.
- Retained and disposed of securely in accordance with legal and professional requirements.

The organisation will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality, the Caldicott Principles, the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, Care Quality Commission Fundamental Standards and all other relevant legislation, professional guidance and contractual requirements.

Information governance is everyone's responsibility. Every individual representing BloodWorks is expected to understand their responsibilities, maintain the confidentiality of

information entrusted to them and contribute to a culture of openness, accountability and continual improvement.

---

2. Purpose

This policy aims to:

- Protect the confidentiality, integrity and availability of all information held by BloodWorks.
- Ensure compliance with UK GDPR, the Data Protection Act 2018 and other relevant legislation.
- Promote safe, lawful and proportionate collection, use, storage and sharing of information.
- Maintain the trust and confidence of clients, staff, partner organisations and the wider public.
- Support the delivery of safe, effective and person-centred healthcare.
- Ensure information governance arrangements support BloodWorks' expanding clinical services, community delivery model and partnership working.
- Define clear responsibilities for everyone handling information on behalf of BloodWorks.
- Promote continual learning and improvement through effective governance and information security.

---

3. Scope

This policy applies to all information created, received, processed, shared or retained by BloodWorks, regardless of format or location.

It applies to all employees, directors, registered professionals, prescribers, associate clinicians, subcontractors, volunteers, contractors, students, agency workers and anyone acting on behalf of BloodWorks.

The policy applies to information relating to, but not limited to:

- Clients and patients.
- Staff and workforce records.
- Volunteers.
- Contractors and subcontractors.
- Partner organisations.
- Clinical records.
- Laboratory results.
- Prescribing records.
- Diagnostic and screening information.
- Financial and contractual information.

- Human resources records.
- Governance documentation.
- Digital communications.
- Photographs, recordings and images where these contain personal information.

It applies equally to information processed within:

- Clinical settings.
- Community health hubs.
- Outreach and mobile services.
- Workplace health programmes.
- Remote and home working environments.
- Microsoft 365 and SharePoint.
- Clinical systems.
- Approved cloud-based platforms.
- Partner organisations acting on behalf of BloodWorks.

This policy should be read alongside all associated BloodWorks governance policies relating to consent, clinical governance, data retention, safeguarding, incident reporting, records management and cybersecurity.

---

4. Information Governance and Confidentiality

Information Governance Principles

Information governance underpins every aspect of BloodWorks' clinical, operational and corporate activity. The organisation is committed to ensuring that information is managed safely throughout its entire lifecycle, from the point it is collected until its secure disposal.

BloodWorks applies the following principles to all personal and organisational information:

- Information will be collected lawfully, fairly and transparently.
- Only information that is necessary for the intended purpose will be collected.
- Information will be accurate, relevant and kept up to date where reasonably practicable.
- Confidentiality will be maintained at all times.
- Information will be protected against unauthorised access, loss, alteration or disclosure.
- Information will be retained only for as long as necessary and disposed of securely.
- Compliance with information governance requirements will be monitored through audit, training and continual improvement.

These principles apply equally to information held electronically, on paper, verbally communicated or otherwise recorded.

Confidentiality

Confidentiality is fundamental to the relationship between BloodWorks and the people who use its services.

Many individuals accessing BloodWorks have chosen to engage because they trust the organisation to provide respectful, non-judgemental healthcare. This includes people accessing preventative healthcare, hormone services, weight management, harm reduction, recovery support and community health services, including individuals who may have experienced stigma or barriers to accessing mainstream healthcare. Protecting confidentiality is therefore essential to maintaining that trust and encouraging continued engagement with healthcare.

Everyone representing BloodWorks has a professional and legal responsibility to protect confidential information obtained during the course of their work.

Confidential information must only be accessed where there is a legitimate work-related reason and must never be discussed with individuals who do not have an authorised need to know.

The duty of confidentiality continues after employment, volunteering or contractual arrangements with BloodWorks have ended.

The Caldicott Principles

BloodWorks applies the Caldicott Principles whenever confidential information is collected, accessed or shared.

In practice this means:

- Confidential information will only be used where there is a justified purpose.
- The minimum necessary information will be used and shared.
- Access to confidential information will be limited to those with a legitimate role.
- Everyone handling confidential information understands their responsibilities.
- Information sharing decisions will balance the duty to protect confidentiality with the duty to provide safe, effective care.
- Information will only be shared where there is an appropriate legal basis or where consent has been obtained, unless another lawful exemption applies.

Collecting Information

BloodWorks collects personal information only where it is necessary to deliver safe, effective and person-centred services.

Depending upon the service being provided, information collected may include:

- Personal identifiers.
- Contact details.
- Relevant medical history.
- Lifestyle information.
- Medication history.
- Laboratory and diagnostic results.
- Prescribing information.
- Consultation records.
- Consent records.
- Payment information.
- Safeguarding information where appropriate.

The amount of information collected will always be proportionate to the service being delivered.

For example, a client attending for community health education or a wellbeing event may provide only minimal personal information, whereas a client receiving regulated clinical assessment, prescribing or ongoing monitoring will require a more comprehensive clinical record.

This proportionate approach reflects BloodWorks' commitment to person-centred care, equitable access and the UK GDPR principle of data minimisation.

Using Information

Information is used only for legitimate healthcare, operational or legal purposes.

Examples include:

- Delivering diagnostic and screening services.
- Clinical assessment.
- Safe prescribing.
- Monitoring treatment outcomes.
- Producing health reports.
- Clinical audit.
- Safeguarding.
- Incident investigation.
- Quality improvement.
- Regulatory compliance.
- Service evaluation.

Information will not be used for purposes incompatible with those for which it was originally collected unless another lawful basis exists or additional consent has been obtained.

Sharing Information

BloodWorks believes that effective information sharing is an important part of safe healthcare. However, information sharing must always be proportionate, justified and lawful.

Information may be shared with:

- The individual concerned.
- General Practitioners.
- Pharmacies.
- UKAS-accredited laboratories.
- NHS organisations.
- Specialist clinicians.
- Community healthcare providers.
- Recovery and voluntary sector partners.
- Criminal justice organisations where appropriate.
- Regulatory bodies.
- Insurers or legal representatives where required.

Most information sharing takes place with the individual's knowledge and, where appropriate, their consent.

Information may also be shared without consent where there is:

- A legal obligation.
- A safeguarding concern.
- A serious risk to the individual or another person.
- A court order.
- An overriding public interest.
- Another lawful basis under UK GDPR or other relevant legislation.

Only the minimum information necessary for the stated purpose will be disclosed.

Information Security

BloodWorks uses appropriate technical and organisational measures to protect the confidentiality, integrity and availability of information.

These include:

- Microsoft 365 and SharePoint.

- Role-based access controls.
- Multi-factor authentication where available.
- Encryption during storage and transmission.
- Secure passwords.
- Device security.
- Secure backup arrangements.
- Regular software updates.
- Restricted administrative permissions.
- Physical security of equipment and premises.

Only approved systems may be used for storing or processing confidential information.

Personal email accounts, unauthorised cloud storage, unsecured messaging applications and removable media must not be used for confidential information unless specifically authorised under organisational procedures.

Community, Outreach and Mobile Working

BloodWorks recognises that healthcare is increasingly delivered outside traditional clinical environments.

Information governance standards therefore apply equally within:

- Community health hubs.
- Mobile clinics.
- Outreach programmes.
- Workplace health initiatives.
- Partnership venues.
- Remote consultations.
- Home working arrangements.

When working away from permanent premises, staff must ensure that:

- Devices remain under their control.
- Screens cannot be viewed by unauthorised individuals.
- Conversations cannot be overheard.
- Paper records are avoided wherever possible.
- Information is uploaded to approved systems at the earliest opportunity.
- Confidential information is never left unattended within vehicles or public places.

Digital Communication

Electronic communication forms an essential part of BloodWorks' service delivery.

Where confidential information is communicated electronically, staff must use approved systems and appropriate security measures.

Before sending confidential information, staff should verify:

- The recipient's identity.
- The recipient's contact details.
- That the information being shared is necessary.
- That an appropriate lawful basis exists.

Particular care should be taken when communicating laboratory results, prescribing information or other clinically sensitive material.

Working with Partner Organisations

BloodWorks works with a number of approved third-party providers to support the delivery of its services. These may include laboratories, pharmacies, prescribing providers, clinical software providers, diagnostic partners and other contracted organisations. Where these organisations process personal information on behalf of BloodWorks, appropriate Data Processing Agreements and contractual arrangements will be in place to ensure information is handled securely and in accordance with applicable legislation.

Records Management

Clinical and organisational records must:

- Be accurate.
- Be factual.
- Be contemporaneous wherever reasonably practicable.
- Clearly identify the author where appropriate.
- Be stored securely.
- Be retained in accordance with the BloodWorks Data Retention and Records Management Policy.

Records must never be altered or destroyed inappropriately.

Where amendments are required, they should be made in a way that preserves the integrity of the original record while clearly identifying the correction.

5. Failure to Comply

Failure to comply with this policy may place individuals, colleagues, partner organisations and BloodWorks at significant legal, clinical and reputational risk.

Breaches of information governance may compromise confidentiality, undermine public confidence, disrupt clinical services and expose individuals to unnecessary harm.

All actual or suspected breaches of confidentiality, information security or data protection must be reported immediately in accordance with the BloodWorks Incident Reporting and Learning Policy.

Examples of serious breaches include:

- Accessing records without a legitimate work-related reason.
- Sharing confidential information without an appropriate lawful basis.
- Discussing confidential information in public or inappropriate settings.
- Sending confidential information to the wrong recipient.
- Using unauthorised devices or systems to store confidential information.
- Failing to report a suspected data breach.
- Deliberately altering, deleting or concealing records.
- Loss or theft of devices containing confidential information.
- Failure to follow BloodWorks policies relating to information security.

Breaches will be investigated proportionately and may result in:

- Additional supervision or training.
- Management action.
- Disciplinary action.
- Removal of system access.
- Termination of employment or contractual arrangements.
- Referral to a professional regulator.
- Notification to the Information Commissioner's Office (ICO), Care Quality Commission (CQC) or other statutory bodies where required.

Where criminal activity is suspected, BloodWorks will cooperate fully with law enforcement agencies.

---

6. Responsibilities

Director

The Director has overall accountability for ensuring that BloodWorks maintains effective information governance arrangements.

Responsibilities include:

- Promoting a culture of confidentiality, transparency and accountability.

- Ensuring sufficient resources are available to support information governance.
- Ensuring appropriate governance systems are maintained.
- Receiving assurance regarding significant information governance risks.
- Supporting continual improvement.

Data Protection Lead

The Data Protection Lead has operational responsibility for overseeing compliance with information governance legislation and organisational policy.

Responsibilities include:

- Providing advice and guidance on information governance matters.
- Monitoring compliance with UK GDPR and the Data Protection Act 2018.
- Managing Subject Access Requests and other information rights requests.
- Investigating information security incidents and data breaches.
- Determining whether incidents require notification to the Information Commissioner's Office.
- Maintaining information governance policies and procedures.
- Supporting staff with complex confidentiality or information-sharing decisions.
- Monitoring training compliance.
- Supporting audits and quality improvement.

Registered Manager

The Registered Manager is responsible for ensuring that information governance is embedded within day-to-day clinical practice.

Responsibilities include:

- Ensuring staff understand their responsibilities.
- Monitoring compliance with organisational policies.
- Supporting safe information sharing.
- Ensuring appropriate record keeping.
- Escalating significant risks or incidents.
- Promoting learning following incidents or audits.
- Supporting quality improvement activities.

Everyone Representing BloodWorks

Every person working on behalf of BloodWorks is personally responsible for protecting confidential information.

Everyone must:

- Comply with this policy and associated procedures.
- Access information only where there is a legitimate work-related reason.
- Protect passwords, devices and system access.
- Maintain confidentiality during and after their involvement with BloodWorks.
- Record information accurately and professionally.
- Report suspected breaches or security concerns immediately.
- Complete mandatory Information Governance training.
- Seek advice whenever unsure whether information should be shared.

Information governance is not solely the responsibility of managers or senior clinicians—it is a responsibility shared by everyone representing BloodWorks.

---

7. Monitoring and Review

Compliance with this policy will be monitored through:

- Clinical governance meetings.
- Information governance audits.
- Clinical record audits.
- Access log monitoring where available.
- Incident reporting and investigation.
- Data breach reviews.
- Subject Access Request monitoring.
- Complaints and compliments.
- Workforce supervision.
- Mandatory training compliance.
- Quality assurance activities.
- Policy review.

Learning arising from audits, incidents, complaints, compliments, changes in legislation and national guidance will be incorporated into service improvement and workforce development.

This policy will be reviewed annually, or sooner where:

- Legislation changes.
- Regulatory requirements change.
- New technologies or digital systems are introduced.
- New clinical services are developed.
- Significant incidents identify a need for review.
- Organisational learning indicates improvements are required.

Related Policies

- Clinical Governance and Risk Management Policy
- Data Retention and Records Management Policy
- Consent Policy
- Collection of GP Details Policy
- Results Communication and Referral Policy
- Cyber Security and Acceptable Use Policy
- Incident Reporting and Learning Policy
- Safeguarding Adults and Children Policy
- Duty of Candour Policy
- Equality, Diversity and Inclusion Policy
- Complaints, Comments and Feedback Policy
- Lone Working Policy
- Medicines Management Policy

References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Care Quality Commission Fundamental Standards
- CQC Regulation 17 – Good Governance
- CQC Regulation 9 – Person-Centred Care
- CQC Regulation 10 – Dignity and Respect
- CQC Regulation 12 – Safe Care and Treatment
- Common Law Duty of Confidentiality
- Caldicott Principles
- NHS Data Security and Protection Toolkit
- Information Commissioner's Office – Guide to UK GDPR
- Health and Social Care (Safety and Quality) Act 2015

BloodWorks Ltd

Records Management and Data Retention Policy

Document Information

Policy Title	Records Management and Data Retention Policy
Policy Category	Governance
Policy Owner	Registered Manager
Approved By	Director and Senior Responsible Officer
Version	2.0
Approval Date	30.07.26
Review Date	30.07.27
Review Frequency	Annual
Applies To	All employees, directors, self-employed practitioners, subcontractors, associate clinicians, volunteers, contractors, agency workers and anyone representing BloodWorks
Status	Draft

Records Management at a Glance

Our Commitment

Accuracy – Integrity • Accountability • Continuity

Security – Protection • Confidentiality • Accessibility

Compliance – Retention • Disposal • Governance

Always

✓ Create accurate and contemporaneous records.

✓ Store records securely using approved systems.

✓ Retain records only for as long as necessary.

✓ Dispose of records securely when no longer required.

✓ Protect records from unauthorised access, loss or alteration.

✓ Follow BloodWorks retention and disposal requirements.

Never

✗ Create false or misleading records.

✗ Store records in unauthorised locations.

✗ Alter or destroy records inappropriately.

✗ Keep records longer than necessary.

✗ Dispose of records using insecure methods.

✗ Remove records without authorisation.

If you're unsure...

Registered Manager

↓

Director / Senior Responsible Officer

1. Statement of Intent

BloodWorks Ltd is committed to maintaining accurate, secure and reliable records that support safe, effective and person-centred healthcare.

Clinical and organisational records provide evidence of the services delivered, support continuity of care, demonstrate accountability and enable BloodWorks to meet its legal, regulatory and contractual responsibilities.

Records will be created, maintained, stored, retained and disposed of in a consistent and secure manner throughout their lifecycle. BloodWorks will retain records only for as long as necessary to meet applicable clinical, legal, regulatory and business requirements before ensuring their secure disposal.

The organisation delivers services directly and through approved partner organisations, including laboratories, prescribing providers, pharmacy partners, diagnostic providers and clinical software suppliers. Where records are created, processed or stored on behalf of BloodWorks, appropriate contractual arrangements will ensure they are managed in accordance with legal requirements and BloodWorks governance standards.

---

2. Purpose

This policy aims to:

- Ensure records are managed consistently throughout their lifecycle.
- Support safe, effective and accountable service delivery.
- Protect the integrity, security and availability of records.
- Establish clear arrangements for record retention and secure disposal.
- Support compliance with legal, regulatory and contractual requirements.
- Promote effective governance across all BloodWorks services.

---

3. Scope

This policy applies to all records created, received, maintained or processed on behalf of BloodWorks.

It applies to records held electronically, in paper format where applicable, and by approved third-party providers acting on behalf of BloodWorks, including laboratories, prescribing providers, pharmacy partners, diagnostic providers and clinical software suppliers.

The policy applies to records including:

- Clinical records.
- Laboratory and diagnostic reports.

- Consultation and prescribing records.
- Consent documentation.
- Governance documentation.
- Incident and audit records.
- Staff and training records.
- Financial and contractual records.

It applies to all employees, directors, self-employed practitioners, subcontractors, associate clinicians, volunteers, contractors, agency workers and anyone representing BloodWorks.

---

4. Records Management and Data Retention

Record Creation

BloodWorks creates and maintains records that support safe, effective and accountable service delivery.

Records should be accurate, factual, contemporaneous and relevant to the service provided. They should clearly document clinical care, professional decisions, organisational activity and any actions taken.

Records must be created and maintained in accordance with professional standards and BloodWorks governance arrangements.

Storage and Security

Records will be stored securely using approved BloodWorks systems and processes.

Access to records will be restricted to authorised individuals who have a legitimate need to access the information in order to carry out their role.

Where records are created, processed or stored by approved partner organisations acting on behalf of BloodWorks, including laboratories, prescribing providers, pharmacy partners, diagnostic providers or clinical software suppliers, appropriate contractual arrangements will ensure records remain secure and are managed in accordance with legal, regulatory and organisational requirements.

Record Retention

Records will be retained only for as long as necessary to meet clinical, legal, regulatory and contractual requirements.

Retention periods will reflect current legislation, recognised guidance and the operational needs of BloodWorks.

Where records become subject to investigation, safeguarding processes, legal proceedings or regulatory review, disposal may be suspended until the matter has concluded.

Standard Retention Schedule

Record Type	Minimum Retention Period
Clinical records, laboratory reports and prescribing records	7 years
Consent documentation	7 years
Incident and complaint records	10 years
Governance records	10 years
Contracts and service agreements	6 years after expiry
Financial records	6 years
Staff records	6 years after employment ends
Training records	Duration of employment plus 6 years
CCTV (where applicable)	30 days unless required for investigation

Secure Disposal

Records reaching the end of their retention period will be disposed of securely in a manner appropriate to the format of the record.

Electronic records will be securely deleted from approved systems. Paper records will be destroyed using approved confidential disposal arrangements.

Where records are held by organisations acting on behalf of BloodWorks, secure disposal will be undertaken in accordance with contractual agreements and applicable legal requirements.

---

5. Failure to Comply

Failure to comply with this policy may compromise clinical governance, confidentiality, continuity of care or regulatory compliance.

Employees who fail to follow this policy may be subject to management or disciplinary action.

Serious breaches may include the creation of inaccurate records, unauthorised access to records, inappropriate alteration or destruction of records, failure to comply with retention requirements or insecure disposal of confidential information.

6. Responsibilities

Director

- Ensure effective records management arrangements are in place.
- Receive assurance regarding records management and compliance.
- Promote good governance across BloodWorks.

Registered Manager

- Maintain oversight of records management practices.
- Ensure records are managed in accordance with this policy.
- Monitor incidents, audits and learning relating to records management.
- Ensure staff receive appropriate training where required.

Everyone Representing BloodWorks

- Create accurate and timely records.
- Maintain records securely.
- Protect confidential information.
- Follow approved retention and disposal arrangements.
- Report any concerns relating to records management.

7. Monitoring and Review

Compliance with this policy will be monitored through:

- Governance meetings.
- Clinical audit.
- Information governance audit.
- Incident reporting.
- Complaints and feedback.
- Quality assurance activities.
- Policy review.

This policy will be reviewed annually or sooner where legislation, organisational change or developments in clinical practice require.

Related Policies

- Information Governance, Confidentiality and Data Protection Policy
- Consent Policy

- Clinical Governance and Risk Management Policy
- Results Communication and Referral Policy
- Incident Reporting and Learning Policy
- Safeguarding Adults and Children Policy
- Cyber Security and Acceptable Use Policy

References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Care Quality Commission Fundamental Standards
- NHS Records Management Code of Practice
- Information Commissioner's Office Guidance on Records Management and Retention