Issue Date: *August 2026*

Review Date: *August 2027*

Lead Officer: Roxy Durran (Quality and Compliance Manager)

Cornwall Neighbourhoods for Change (CN4C)

Records Management Policy

1. Purpose

Cornwall Neighbourhoods for Change (CN4C) is committed to creating, maintaining and managing accurate, reliable and secure records to support the effective delivery of services, safeguard individuals, demonstrate accountability and comply with legal and regulatory requirements.

This policy sets out the principles and responsibilities for the creation, storage, maintenance, retention, retrieval, sharing and disposal of organisational records across all areas of CN4C.

Effective records management supports good governance, protects personal information, enables informed decision making and ensures that records remain accessible, accurate and secure throughout their lifecycle.

2. Links to Other Policies

This policy should be read alongside:

- Data Protection Policy
- Information Sharing Procedure
- Safeguarding Policy
- Low-Level Concerns Policy
- Complaints Policy
- Health and Safety Policy
- Information Security Policy
- Acceptable Use of IT Policy
- Business Continuity Plan
- Whistleblowing Policy

Statutory and Regulatory Guidance

This policy reflects the requirements of:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- Freedom of Information Act 2000
- Limitation Act 1980
- Keeping Children Safe in Education (KCSIE), where applicable
- Independent School Standards, where applicable
- Information Commissioner's Office (ICO) Guidance

3. Associated Procedures

- Record Creation Procedure
- Record Retention Procedure
- Secure Disposal Procedure
- Subject Access Request Procedure
- Information Sharing Procedure
- Data Breach Procedure

4. Principles

CN4C is committed to ensuring that all organisational records are:

- Accurate.
- Complete.
- Reliable.
- Accessible to authorised individuals.
- Securely stored.
- Protected against unauthorised access.
- Retained only for as long as necessary.
- Disposed of securely in accordance with legislation.
- Managed in a way that supports the organisation's transition from paper-based to digital record keeping wherever possible, ensuring records remain accessible, secure, efficient and compliant with legislative and regulatory requirements.

Records should support:

- Safe service delivery.
- Good governance.
- Safeguarding.
- Legal compliance.
- Accountability.
- Continuous improvement.

Digital Transition

CN4C is committed to progressively transitioning from paper-based records to secure digital record-keeping systems wherever practicable. This transition aims to improve the accessibility, security, accuracy and efficiency of organisational records while supporting effective information sharing, reducing duplication and promoting environmentally sustainable working practices. Digital records will be managed in accordance with data protection legislation, information governance requirements and organisational procedures to ensure they remain secure, reliable and accessible to authorised individuals.

5. Scope

This policy applies to:

- All employees.
- Volunteers.
- Trustees.
- Agency workers.
- Contractors.
- Consultants.
- Students on placement.
- Anyone creating or managing records on behalf of CN4C.

It applies to records held in:

- Paper format.
- Electronic systems.
- Email.
- Databases.
- Cloud-based systems.
- Photographs.
- Audio recordings.
- Video recordings.
- Mobile devices where authorised.

6. Roles and Responsibilities

Chief Executive Officer (CEO)

The Chief Executive Officer has overall accountability for ensuring that Cornwall Neighbourhoods for Change (CN4C) complies with all relevant legislation, statutory guidance and organisational requirements relating to records management, information governance and data protection.

The Chief Executive Officer will:

- Ensure appropriate records management arrangements are in place across the organisation.
- Promote a culture of accurate, secure, timely and professional record keeping.
- Ensure sufficient resources are available to support effective records management.
- Support the organisation's transition from paper-based to digital records where appropriate.
- Ensure compliance with legal, regulatory and contractual requirements.
- Receive assurance that records management systems are operating effectively.

Senior Leadership Team

The Senior Leadership Team is responsible for ensuring this policy is implemented consistently across all areas of Cornwall Neighbourhoods for Change.

The Senior Leadership Team will:

- Promote good records management practices throughout the organisation.
- Ensure appropriate systems are in place for creating, maintaining, storing and disposing of organisational records.
- Monitor compliance with this policy and associated procedures.
- Ensure managers, coordinators and staff understand their responsibilities.
- Promote the effective use of approved digital record management systems.
- Support continuous improvement in records management and information governance.

Managers and Coordinators

Managers and Coordinators are responsible for ensuring that records within their areas of responsibility are maintained to a high professional standard and managed in accordance with organisational requirements.

Managers and Coordinators will:

- Ensure records are accurate, factual, objective and completed in a timely manner.
- Ensure records are maintained securely and confidentially.
- Review records regularly to ensure they remain current, relevant and complete.
- Ensure records are retained and disposed of in accordance with CN4C's Record Retention Schedule.
- Ensure records are accessible only to authorised individuals.
- Promote the use of approved digital systems and support the organisation's transition from paper-based records wherever practicable.
- Ensure staff comply with this policy and associated procedures.
- Provide staff with appropriate guidance and support in relation to records management.
- Ensure staff complete mandatory Records Management, Information Governance and Data Protection training relevant to their role.
- Monitor staff compliance with mandatory training requirements and ensure refresher training is completed where required.
- Address concerns relating to poor record keeping promptly and implement improvements where necessary.

Person Nominated for Quality Assurance and Compliance

The Person Nominated for Quality Assurance and Compliance is responsible for supporting the effective implementation, monitoring and continuous improvement of records management arrangements across CN4C through quality assurance activities, audits and policy review.

The Person Nominated for Quality Assurance and Compliance will:

- Monitor compliance with this policy and associated procedures.
- Audit the quality, accuracy, completeness and timeliness of organisational records.
- Review compliance with information governance and records management standards.
- Monitor the effective use of approved digital record management systems.
- Identify themes, trends, risks and opportunities for improvement.

- Report findings and recommendations to the Senior Leadership Team.
- Identify training or development needs arising from quality assurance activities.
- Coordinate the scheduled review of this policy.
- Support continuous improvement in records management practices across the organisation.

All Staff

Every member of staff has a responsibility to maintain accurate, timely, professional and confidential records as part of their day-to-day duties.

Staff will:

- Create records that are factual, objective, contemporaneous and accurate.
- Complete records promptly using approved organisational systems.
- Maintain confidentiality and comply with data protection legislation at all times.
- Store records securely using approved organisational systems and processes.
- Only access information required to undertake their role.
- Report any concerns relating to record keeping, confidentiality, information security or data breaches immediately.
- Comply with this policy, associated procedures and relevant legislation.
- Complete all mandatory Records Management, Information Governance and Data Protection training relevant to their role.
- Keep their knowledge and skills up to date by completing refresher training and any additional learning required to support changes in legislation, organisational procedures or digital record management systems.
- Seek advice from their manager where they are unsure of record keeping requirements or responsibilities.

7. Creating Records

Accurate, timely and professional record keeping is essential to the effective operation of Cornwall Neighbourhoods for Change (CN4C). Organisational records provide evidence of decisions, actions and the services delivered and may be relied upon during inspections, audits, safeguarding enquiries, complaints, disciplinary investigations or legal proceedings.

All records created on behalf of CN4C should:

- Be factual, accurate and objective.

- Be completed as soon as reasonably practicable after the event or activity.
- Be clear, concise and written in plain, professional language.
- Be legible and easily understood.
- Include the date and, where appropriate, the time of the record or event.
- Include the name, role or identifiable signature of the person completing the record.
- Clearly distinguish factual information from professional opinion, ensuring any opinions are evidence based and relevant.
- Include only information that is necessary, relevant and proportionate to the purpose of the record.
- Be respectful and appropriate in tone, avoiding discriminatory, emotive or subjective language.
- Be stored using approved organisational systems and formats.

Records should present an accurate account of events and should never be altered, falsified or amended in a way that misrepresents information or conceals the original record.

Where amendments or corrections are necessary, the original entry should remain identifiable where reasonably practicable. Any amendments should be dated, attributable to the person making the amendment and include a brief explanation where appropriate. Electronic records should maintain an appropriate audit trail where systems allow.

Where records relate to safeguarding, health and safety, learner welfare or employment matters, they should be completed promptly to ensure information remains accurate, supports effective decision making and enables appropriate action to be taken where required.

8. Record Storage

Cornwall Neighbourhoods for Change (CN4C) is committed to ensuring that all organisational records are stored securely, remain accessible to authorised individuals when required and are protected against loss, damage, unauthorised access or disclosure.

Records will be stored using approved organisational systems and facilities that are appropriate to the type, sensitivity and purpose of the information being held.

Secure storage arrangements include:

- Password protected electronic systems and databases.
- Role based access permissions to ensure information is only accessible to authorised individuals.

- Secure filing systems for paper records.
- Locked cabinets or storage areas for confidential and sensitive records.
- Encrypted devices and storage media where appropriate.
- Secure cloud-based storage solutions approved by the organisation.
- Regular system backups and recovery arrangements for electronic records.
- Appropriate environmental conditions to protect paper records from damage or deterioration.

Access to records will be restricted to individuals who have a legitimate business or professional need to access the information as part of their role. Staff must only access records that are necessary for the performance of their duties and must never access information without authorisation.

Managers are responsible for ensuring records within their area are stored securely and that appropriate access controls are maintained. Access permissions will be reviewed periodically to ensure they remain appropriate when staff roles or responsibilities change.

Where records are removed from organisational premises for legitimate business purposes, staff remain responsible for ensuring they are transported, stored and used securely in accordance with organisational procedures.

All records will be managed in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, CN4C's Data Protection Policy and Information Security procedures.

9. Record Retention

Cornwall Neighbourhoods for Change (CN4C) is committed to retaining organisational records for appropriate periods of time to support effective service delivery, meet legal and regulatory obligations, protect the rights of individuals and demonstrate organisational accountability.

All records will be retained in accordance with CN4C's Record Retention Schedule and relevant legislative, regulatory and contractual requirements. Retention periods will be determined by considering:

- Legal and statutory requirements.
- Regulatory guidance and best practice.
- Safeguarding responsibilities.
- Operational and business needs.
- Financial and audit requirements.

- Contractual obligations.
- The potential need to support investigations, complaints or legal proceedings.

Records will not be retained for longer than is necessary for the purpose for which they were created. Once the approved retention period has expired, records will be securely disposed of in accordance with the Secure Disposal section of this policy, unless there is a lawful reason to retain them for a longer period.

Managers are responsible for ensuring that records within their areas of responsibility are retained, reviewed and disposed of in accordance with the Record Retention Schedule. The Person Nominated for Quality Assurance will monitor compliance through periodic audits and quality assurance activities.

Where records are required for ongoing safeguarding enquiries, legal proceedings, regulatory investigations, complaints, Freedom of Information requests or Subject Access Requests, they must not be destroyed until all relevant matters have been concluded and any extended retention requirements have been met.

CN4C will review its Record Retention Schedule regularly to ensure it remains compliant with current legislation, regulatory requirements and organisational needs.

10. Secure Disposal

Cornwall Neighbourhoods for Change (CN4C) is committed to ensuring that records containing personal, confidential or commercially sensitive information are disposed of securely once they have reached the end of their approved retention period.

Before any records are destroyed, the appropriate retention period must be confirmed in accordance with CN4C's Record Retention Schedule and any applicable legal, regulatory or contractual requirements. Records must not be destroyed where they are subject to ongoing investigations, litigation, audits, safeguarding enquiries, complaints, Freedom of Information requests or Subject Access Requests.

Records that have reached the end of their retention period will be disposed of using secure methods appropriate to the type of record, including:

- Confidential shredding of paper records.
- Approved secure destruction services.
- Permanent deletion of electronic records from organisational systems.
- Secure destruction of digital storage media where appropriate.
- Secure disposal of portable storage devices in accordance with organisational procedures.

All disposal methods must ensure that information cannot be reconstructed, recovered or accessed by unauthorised individuals.

Managers are responsible for ensuring that records within their area of responsibility are disposed of securely and in accordance with this policy. Where appropriate, a record of disposal should be maintained to demonstrate compliance with organisational and legislative requirements.

The secure disposal of records forms an essential part of CN4C's information governance arrangements and supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation.

11. Record Quality

Cornwall Neighbourhoods for Change (CN4C) is committed to maintaining high quality records that support effective service delivery, safeguarding, governance and informed decision-making.

Managers will regularly review records within their areas of responsibility to ensure they are:

- Accurate and factually correct.
- Up to date and completed within appropriate timescales.
- Complete and contain all relevant information.
- Clear, objective and professionally written.
- Relevant and proportionate to their purpose.
- Stored securely and in accordance with organisational procedures.
- Accessible to authorised individuals when required.
- Retained and managed in accordance with the Record Retention Schedule.

Where inaccuracies, omissions or poor record keeping practices are identified, appropriate corrective action will be taken promptly. This may include updating records, providing feedback to staff, reviewing working practices or implementing additional training where necessary.

The Person Nominated for Quality Assurance will undertake periodic audits and sampling of records to monitor compliance with this policy, identify areas for improvement and promote consistency across the organisation. Findings from these audits will inform Quality Assurance activities, staff development and continuous organisational improvement.

12. Confidentiality

Cornwall Neighbourhoods for Change (CN4C) is committed to maintaining the confidentiality of all personal, sensitive and organisational information. Confidentiality is fundamental to protecting the privacy, dignity and rights of learners, families, staff and partner organisations, whilst supporting safe and effective service delivery.

All records containing personal or sensitive information will be handled with the highest standards of confidentiality and will only be accessed by individuals who have a legitimate need to know in order to carry out their professional responsibilities.

Confidential information will only be accessed, used or shared where there is:

- A legitimate business or professional need.
- A legal or statutory obligation.
- A safeguarding concern or to protect an individual from harm.
- Appropriate consent, where this is the lawful basis for sharing information.
- Another lawful basis under UK GDPR and the Data Protection Act 2018.

Confidential information must only be discussed in appropriate professional settings and should never be disclosed to unauthorised individuals or discussed in public areas where it may be overheard.

Whilst CN4C recognises the importance of confidentiality, it is not absolute. Safeguarding concerns may require CN4C to override confidentiality in exceptional circumstances where it is necessary to protect a child, young person or adult at risk from actual or potential harm**.** Where there are concerns that an individual may be at risk of abuse, neglect, exploitation or other significant harm, or where there is a legal or statutory duty to share information, confidentiality must not prevent appropriate information sharing.

In these circumstances, information will only be shared on a need-to-know basis, ensuring that it is necessary, proportionate, relevant, accurate, timely and secure, and in accordance with the Data Protection Policy, Information Sharing Procedure, Safeguarding Children and Young People Policy and applicable legislation.

All employees, volunteers, contractors and others working on behalf of CN4C are responsible for maintaining confidentiality and protecting the information they access as part of their role. Any actual or suspected breaches of confidentiality must be reported immediately to an appropriate manager and managed in accordance with organisational procedures.

13. Information Security

Cornwall Neighbourhoods for Change (CN4C) is committed to protecting all organisational records and information from loss, unauthorised access, misuse, damage or disclosure. Appropriate technical, physical and organisational measures will be implemented to ensure the confidentiality, integrity and availability of information held by the organisation.

Information security measures will include, but are not limited to:

- Protecting records against loss or accidental destruction.
- Preventing unauthorised access to confidential information.
- Protecting information from theft, misuse or unlawful disclosure.
- Implementing secure password and access control measures.
- Using approved organisational systems for storing and sharing information.
- Protecting records against cyber threats, malware and other security risks.
- Maintaining appropriate backup and recovery arrangements for electronic records.
- Ensuring paper records are stored securely when not in use.
- Regularly reviewing user access permissions to ensure information is only accessible to authorised individuals.

All employees, volunteers and others working on behalf of CN4C are responsible for maintaining information security and must take reasonable steps to protect organisational records and confidential information at all times.

Where safeguarding concerns require information to be shared in order to protect an individual from harm, this will be undertaken lawfully, securely and only with those who have a legitimate need to know. Information security measures must support, and not prevent, appropriate safeguarding information sharing.

Any suspected or actual information security incident, data breach or unauthorised disclosure of information must be reported immediately to an appropriate manager and managed in accordance with the Data Protection Policy and Data Breach Procedure. Prompt reporting enables CN4C to minimise potential risks, meet its legal obligations and implement any necessary corrective actions.

14. Monitoring and Auditing

Record management arrangements will be monitored through:

- Quality Assurance audits.
- Record sampling.
- Data protection audits.
- Safeguarding audits.
- Internal compliance reviews.
- External inspections where applicable.

Audit findings will be used to improve organisational practice.

15. Equality, Diversity and Inclusion

CN4C is committed to ensuring that records are managed fairly, lawfully and without discrimination.

Where appropriate, reasonable adjustments will be made to ensure records are accessible to individuals with disabilities or additional communication needs while maintaining confidentiality and security.

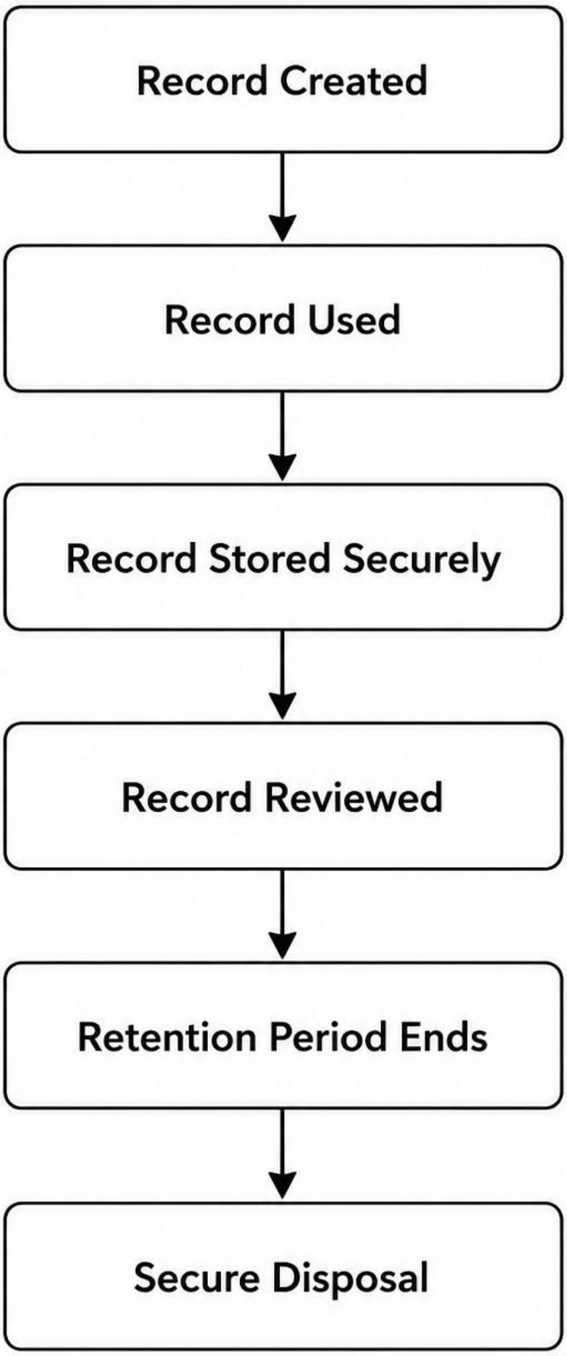
16. Monitoring and Review

This policy will be reviewed annually or sooner following:

- Changes to legislation.
- ICO guidance updates.
- Audit findings.
- Inspection outcomes.
- Significant incidents.
- Lessons learned.

The Chief Executive Officer is responsible for ensuring this policy remains current and compliant.

Appendix 1 - Record Lifecycle



Appendix 2 - Good Record Keeping Checklist

Records completed promptly. ☐

Information is factual and objective. ☐

Dates recorded. ☐

Author identified. ☐

Confidentiality maintained. ☐

Stored securely. ☐

Reviewed where appropriate. ☐

Retention period identified. ☐

Appendix 3 - Record Categories

Record Type	Examples
Governance	Board minutes, policies, strategic plans
Human Resources	Personnel files, recruitment records, supervision records
Finance	Invoices, payroll, budgets, audit records
Health & Safety	Risk assessments, accident reports, fire records
Safeguarding	Safeguarding concerns, referrals, chronologies
Learner Records	EHCPs, ILPs, assessments, attendance, behaviour records
Quality Assurance	Audits, observations, improvement plans, IQA records
Operational	Contracts, service agreements, correspondence

Appendix 4 - Record Retention Principles

Records should be retained only for as long as:

- Required by legislation.
- Required for safeguarding purposes.
- Required for financial or contractual reasons.
- Required to support organisational business.

Once no longer required, records should be securely destroyed in accordance with the Secure Disposal Procedure.

Appendix 5 - Secure Disposal Checklist

Retention period checked. ☐

Authorisation obtained where required. ☐

Records securely destroyed. ☐

Electronic records permanently deleted. ☐

Confidential waste disposed of appropriately. ☐

Disposal recorded where appropriate. ☐