Coventry City Council

Children's Services

Recording Policy

Policy statement

Coventry City Council Children's Services sees good quality recording and record management is an essential part of evidencing the practice and accountability of the Council's staff. It is one of the cornerstones of the development of partnership and good practice. It is an integral part of the service it provides to the children, young people and families we work with.

Promoting the resilience, wellbeing and safeguarding of the children, young people and families we work with requires information to be brought together from a number of sources. Professional judgements and decisions are made on the basis of this information in partnership with the individual children and young people, families, carers and other partners.

This document aims to promote good practice in Children's Service by setting out requirements and standards for recording and records management.

People that need to be assured that our recording is of good quality include:

- Children, young people, their families and carers – good quality recording helps to protect their rights. They should have accurate and evidence based statements of their outcomes, needs and decisions taken in an easily accessible format.

- Staff and colleagues – good quality recording ensures that they have the relevant information available to keep them safe and to help them to work most effectively with children and young people and their families.

- Local Managers – good quality recording helps them to make decisions and to oversee the work done in their teams. It also helps to gain information that will support service development and improvement.

- Senior Managers – good quality recording supports situations when they need to account for agency decisions or in disciplinary or performance investigations.

- Legal Advisors and Insurers – good quality recording can make it possible to present evidence properly and defend challenges against the Council.

- Health, Police, Schools and other contributors – good quality recording means that the information they are supplying is used for its intended purposes only and only used with permission.

CONTENTS

1. Scope and definition of a record'

1.1 This policy outlines the case recording requirements in Coventry City Children's Services and applies to all operational, managerial and administrative staff working with children, young people and their families and carers within Children's Services in Coventry who need to record information about with children, young people, their families and carers citizens and carers.

This includes all staff employed by other organisations and seconded to the Council or who are employed by other organisations and are required to use the Council's systems as part of their role.

1.2 **A Record** is defined in this policy as:

Case recording is the written account of the department's work with and on behalf of an individual, their family or carers

The Local Authority has a responsibility of ensuring that:

- Each child receiving a service has a separate written care record;
- Once a decision has been made to formally consider a child for Adoption, the Adoption pathway will be started on the ICS system. Additionally to this, a paper file will be need to be kept made up of any original documents and papers with birth parents signatures;
- Separate case records are kept for carers being assessed by Children's Specialist Services such as Foster Carers, Special Guardians and Adopters.
- In addition the Local Authority has a responsibility for keeping registers of Foster Carers, children in the care of Foster Carers, and children in residential homes.
- Children and their families have a right to be informed about the records kept on them, the reasons why and their rights to confidentiality and of access to their records. Creation of a Record
- Multiple Records - Across the Council it is possible that one person may have a number of different elements of a record stored at different locations. For the purpose of this policy the person only has one 'record' and it includes all of these parts. Local protocols for merging files and storage remain in place.
- 'Recorded information which identifies a person (child, young person, parent or carer) that has been created, received and maintained by Children's Services while carrying out our work and kept for the purpose of that work'. Records covered include:

  Children's Case files;
  Foster Carers and potential Foster Carers case files;

Child's Adoption case record;
Adopters and potential adopters case files;
Special Guardians and potential Special Guardians case files;
Post Adoption, post Special Guardian support case records;
The records apply to hard copy and electronic records

1.3 A record can include:

- Paper based records such as logs, minutes, correspondence etc.
- Electronic Records (e.g. Protocol ICS or ECAF)
- E-mail and attachments such as Word documents
- Removable/portable digital media including memory sticks, DVD and CDs.
- Complaints Records
- Information received in any form from external sources.
- Photographs
- CCTV

The case records are primarily for the benefit of the child, parent or carer and should be an accurate reflection of the individual person's life. It is a record between the individual and the department not an individual member of staff's record;

Recording details the individual worker's contact with the individual and others, the work to be done and its objectives, the procedures followed, the assessment of need, decisions about eligibility, the Care Plan, the provision of services, the timing, process and outcomes of monitoring and reviews;

Recording draws on information and knowledge from a wide range of sources, including partners and other agency policies;

Recording includes description, analysis and professional judgement. It is essential that a distinction is made between fact and opinion and where there is a third party contribution.

Personal Data is defined as all information which personal identifies the service user. This could be name, address, date of birth, unique reference numbers.

Sensitive personal data is defined as information which relates to a person's: race/ethnicity, political opinion, religious beliefs (or similar), physical or mental health or condition, sexual life, commission of offences (including alleged), proceedings for any offence committed (including alleged).

Both types of data relate to that held in any format, eg emails, electronic records, paper records, CCTV includes all information which personally identifies the that relates to an individual service user.

The data held on the Council's service user electronic information systems includes records of personal sensitive personal details, such as name, address,

date of birth, and ethnicity. It also includes contact, enquiries, referrals, assessments, plans, panel decisions, services delivered and financial transactions. Any photo, audio or video recordings of work undertaken also form part of this case record.

2. Purpose of recording

The overall purpose of recording is to demonstrate and enable the work of the department in the assessment and provision of services, for monitoring and reviewing and also to show the needs of individuals who may require or who are receiving a service. Recording also documents the staff that provides the service in order for them to be accountable for their work.

Good case recording (both electronic data systems and paper files) enables:

- An accurate account of the work of the department with the individual, their family, carers, other relevant people and care providers to be maintained;
- Enables children and young people to understand their journey and care history where their story can be told about their life that provides a balanced picture of particular events and includes both positive and negative incidents;
- Allows an individual, particularly a child, to look back at their life and recall clearly or where they may not have known all the facts, about at that time and the reasons for certain decisions;
- A record to be made of important things in a person's life that may be necessary to explain to him/her at a later date;
- A record to be made of the views of individuals and their family members;
- The department to account in terms of the work that has been undertaken;
- Partner Agencies, where appropriate, to share accurate information;
- Evidence to be available of compliance with relevant legislation and departmental policies and procedures;
- Evidences and supports effective partnerships with children, young people, their families and carers
- Staff to be able to reflect back on work undertaken, risk assessments, decision making process and plan any future intervention.
- Continuity in service being provided when staff change;

- Becomes a source of evidence for investigation and accurate information to be provided as evidence in Court, enquiries, access to information requests, complaints or legal challenge

- The production of accurate business information for performance management and quality assurance purposes.

- Provides an essential tool for managers to monitor work and ensure compliance with departmental policies and procedures

- Meet the Council's legal duties and responsibilities

3. Legal and Professional Context

3.1 This document supports staff and the department to comply with the various requirements and guidance set out in:

- The Data Protection Act (1998)
- The Caldicott Principles (1997 and as amended in 2013)
- The Freedom of Information Act (2000)
- Children Act 1989
- Children Act 2004
- Achieving Best Evidence (Ministry of Justice 2011)
- The Equalities Act (2010)
- The Human Rights Act (1998)
- The Mental Capacity Act (2005)
- Coventry Information Sharing Protocol
- Working Together 2015
- Council policies and standards as set out in its Information Security
- Management Framework

3.2 All staff must comply with guidance from their own professional bodies

Health and Care Professions Council Standards of Conduct, Performance and Ethics (2008).

The tenth standard states that "*You must keep accurate records…Making and keeping records is an essential part of care and you must keep records for everyone who asks for your advice or services. You must complete all records promptly. You must protect information from being lost, damaged or accessed by someone who does not have the appropriate authority, or tampered with."*

Professional Capabilities Framework for Social Workers (2012)

Social Workers should be able to "*Record information in a timely and accurate manner. Write records and reports for a variety of purposes with language suited to function using information management systems. Distinguish fact from opinion*

and record conflicting views and perspectives. Clearly report and record analysis and judgements"

4. Standards for all records (Paper or Electronic)

If it is not recorded it did not happen

1. Timeliness of recording

- Records should be completed by the person undertaking the tasks **within 2 working days or in line with the relevant statutory guidance.**

- All records of events must be written at the time of or as soon as possible after the events to which they relate. Where work is undertaken to assess whether a child, young person or adult may be at risk of significant harm, or to protect them from this, all relevant information must be recorded if at all possible within the **same working day** and at the **latest within 24 hours**.

2. Records and consent to information sharing decisions

- Staff must ensure that Children, Young People and their families are aware that records will be created and kept about them, the reason for keeping such records, how their information will be used and possibly shared.

- Consent to share information should be agreed and the 'consent for information sharing' document or any other type of fair processing notice should be signed and added to the record

- Ensure that there is a record of any documents shared, with whom, for what purpose and when.

- There are circumstances where it may not be appropriate to inform the user at the time of disclosure, for example police investigations or where the safety of a child or adult may be compromised. Any decisions to delay informing users should also be written in the record stating the reason why and the name of the person making that decision.

- If consent has not been gained or you are in any doubt whether to disclose information please consult with your manager and if necessary seek advice from the Information Governance Team. Further information and advice is contained in the Coventry Information Sharing Protocol.

3. Records should be accurate

- Recording must be accurate, appropriate, timely, with all sources of information identified;

- All records must be written in the context of the individual that the entry is about (or their legal representative/advocate), that they could see the entry at any time or the record could be used as evidence in Court;

- All individual pieces of paper must be identified with the individual's name, and date of birth / and electronic case record number;

- Case files for children must clearly identify who has Parental Responsibility for the child;

- All records must contain the date and time that the entries were made and the narrative contain the date and time that any events occurred.

- All entries on paper records must be signed with the staff's name printed underneath;

- All entries must be written, wherever possible, in terms which the child or family members will be able to understand;

- When it is a significant event the tick box must be selected on the ICS case note to allow this to be pulled through to the chronology and edited to ensure that it is succinct and relevant

4. Records should be easy for people to access and understand

- Records must be written concisely, in plain English, with correct spelling and grammar, and must not contain any expressions that might give offence to any individual or group;

- Use of jargon, technical or professional terms and abbreviations must be kept to a minimum. If there is likely to be any doubt, they must be defined;

- Electronic communications i.e. emails between professionals relating to a person's care must be included in the case records;

- All documents and reports must be signed and dated by the person writing the report, their position and the date of the report;

- All hand written records must be written legibly and indelibly in black ink;

- Where hand written records / notes are typed into a report / minutes of a meeting or entered into database the date that the contemporaneous notes were taken must be used for the recording.

- If there is an electronic recording system in place it must be used. This includes scanning in documents received and any signatures gained.

- Information should be produced or communicated in a way that meets any specific communication needs of the person receiving it.

5. Records should be concise and relevant

- Records must be clear and unambiguous;

- Records need to be proportionate and sufficient to fulfil our roles within Children's Services. There is a need to balance keeping notes brief and to the point with making sure we record the key information we need to.

- Recording should capture enough information to be useful if needed at a later date. The purpose and context of the activity should guide the length and detail of the recording.

- Any correction or amendments to inaccurate information must be agreed by first line managers, who should record their agreement to action being taken to correct but not remove the record.

- Original records should not be altered or erased. If amendments or additions are needed these should make it clear where a change has been made with the date/ signature and leave visible the information which has been corrected. Where the inaccurate information has been passed on to others, then they must also informed.

- Tippex should not be used and blank spaces should be crossed out Amendments or additions should end with the name and role of the person that has made them and the date the amendment was made (and signature when handwritten).

- The agreed change should be noted in the Case Notes and also wherever the information occurs in the case record. This includes both the paper and file and the computer based record.

- Wherever possible and appropriate the content of records should be shared with the individual it is about; If an individual disagrees with the record this must be recorded;

6. **Records should distinguish fact, opinion and hearsay.**

Fact – Information that is accurate and direct observations of events.

Opinion - An opinion is a view expressed about the significance of information or interpretation of behaviour or events that have been observed. Where opinions are recorded it is important to be clear about the factual basis for any opinion, include any available information about the basis on which they are made and ensure this is within the limits of your expertise.

Hearsay - information told to you by others, which are relevant to the case but which you cannot personally verify.

7. Recording should support Equalities and Anti-Discriminatory Practice.

- Record with respect and sensitivity to difference in culture, language, ethnicity, race, age, gender, disability, sexual orientation, religion and sensory impairment.

- Be aware of and avoid language that stereotypes or labels people. Where descriptive words such as 'aggressive' are attributed, these need to be supported with evidence and information to explain how this description has arrived at.

8. Records should be kept securely and accessed appropriately

- All records held on children must be kept securely.

- Children's paper files and other day-to-day records should be managed securely normally be stored in a locked cabinet, or a similar manner, usually in an office which only staff/carers have access to.

- These records should not be left unattended when not in their normal location.

- Only allowing authorised people into Council premises or restricted areas

- Ensuring visitors are escorted whilst in Council premises

- All electronic records must be kept securely and this will include arrangements such as:

  Making sure ICT equipment is secure and logged out when left unattended
  Password protection and changing passwords on a regular basis.

More information on information security and management can be found in the Council's Standard for Acceptable Use of Computer, Internet & Email Facilities can be found at: http://beacon.coventry.gov.uk

9. Records are reviewed regularly and audited

Supervisors and Managers at all levels are responsible will regularly for overseeing the quality of case recording within the service through the supervision process, quality assurance audits and when signing off documents and records.

5. Confidentiality and sharing information

1. Confidentiality and Consent

Staff should not pass confidential information or documents to any outside person or organisation unless you have prior permission to do so from the data subject (e.g. people who use services, carers or organisations). If information was supplied by a third party (e.g. Health Professional or family friend) then consent should be obtained from that individual.

For workers based in multi-agency and multi-disciplinary teams, local information sharing protocols must be in place and applied in practice.

2. Information sharing without consent

In cases where consent has not be obtained the Council requires lawful grounds to override consent. For example:

- If an individual is believed to be at serious risk of harm, or
- If there is evidence of serious public harm or risk of harm to others, or
- If there is evidence of a serious health risk to an individual, or
- If the non-disclosure of information would significantly prejudice the prevention, detection or prosecution of a crime, or
- If instructed to do so by a court
- As part of a best interest decision relating to sharing information if the person does not have the capacity to consent under the Mental Capacity Act (2005).
- An Independent Mental Capacity Advocate has satisfied the relevant requirements to access information without consent.

Where information sharing is being considered without consent it is important staff discuss this with their line manager and if required seek advice from the Council's Caldicott Guardian, before a disclosure is made.

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service-user information and enabling appropriate information-sharing across health, social care and other partner agencies.

If it is agreed it is appropriate to share information without consent then the information must be relevant for the purpose for which it is being shared and be accurate at the time of disclosure.

It is important to remember to disclose the minimum amount of information. It is also important that the information is shared securely.

Where information is shared without consent this should be recorded outlining the rational for this decision and how the information was shared.

3. Information classifications for information sharing

When sharing any personal or sensitive information both internally and externally it is important to ensure information is classified correctly. The Council has adopted the Central Government's Classification Standard – 'Official', 'Official Sensitive', 'Secret', and 'Top Secret'. The majority of information within the Council will be:

- Official
- Official Sensitive

Definitions:

OFFICIAL – All routine public sector business, operations and services should be treated as OFFICIAL.

OFFICIAL Sensitive – This information can be business and/or personal information, which if lost or stolen could result in significant impact on the Council, other organisations or individuals (e.g. personal, sensitive personal data, such as Subject Access Requests, case management documents, minutes from Safeguarding meetings).

More information is available within the Council's standard for Information Classification located on the Intranet:

http://beacon.coventry.gov.uk/downloads/file/724/standard_for_information_classification

If you are unsure as to what classification you need to apply or have any queries, please contact the Information Governance Team at infogov@coventry.gov.uk

If e-mails containing personal and sensitive information outside of a secure system need to be sent please ensure that documents are password protected.

Request that the recipient makes contact via the telephone to obtain the password. On the rare occasions when this is not possible, ask the recipient to confirm receipt by return and send the password separately. The password needs to be individual to that document.

4. Subject access to records

Both the Data Protection Act 1998 and the Freedom of Information Act 2000 provide legal avenues for people to obtain information that the Council holds

The Data Protection Act applies to both paper and manual records and records held electronically. It is important that electronic recording systems comply with the requirements for children and their families to easily find their story in a logical narrative.

The Freedom of Information Act 2000 gives people the right to see all types of other non-personal information held by children's services. Local authorities should publicise their access to records policy with clear information about how care leavers and others can apply for their records and access support services.

5. Data Protection Act (1998) – Subject Access Requests

Under Section 7 of the Data Protection Act (1998) any person who is the subject of personal information held by the Council, has a right of access to this information. Requests of this nature are called Subject Access Requests.

Staff must inform the Council's Information Governance Team (IGT) if they receive a Subject Access Request.

The IGT team will then allocate a unique reference number and send out a request form and a letter, outlining the next steps that a requester needs to take. The requester has to pay a statutory fee to access their information.

Once the requester has paid the required fee the Council has 40 calendar days to analyse, prepare and disclose the information.

Requesters are only entitled to information about themselves. Any personal information about another person (third party) must be removed (redacted) before disclosure is made, unless written consent is given by the third party or it is reasonable, in the circumstances, to disclose it.

Additionally, any information owned by another organisation (Police, Courts, other authorities etc) must also be removed, unless their consent can be obtained, or again it is reasonable in the circumstances.

Further information on the Data Protection Act 1998 can be found on the intranet at:
http://beacon.coventry.gov.uk/downloads/download/243/data_protection_policy

6. Freedom of Information Act (2000)

The Freedom of Information Act (2000) applies to all public authorities, including Coventry City Council. It allows anyone to request information on any function of the Council.

Requests could be to see any information recorded, stored or managed by or on behalf of the Council. This includes letters, notes, e-mails, minutes from meetings, maps, CCTV tapes, post-it notes, plans, photographs and database records etc. It also includes other information sent to us from other organisations (including partner organisations or the private sector).

There are a number of FOI exemptions for non disclosure of information. In order to withhold information it will be necessary to be able to cite one of the exemptions or exceptions in accordance with the legislation.

The Council's Information Governance Team (IGT) provides advice and support in dealing with information requests; alternatively each Directorate of the Council has a Lead Officer specialising in Information Governance. In Community Services queries should be directed to the Caldicott Guardian.

Further information about the Freedom of Information Act 2000 can be found on the intranet at:
http://beacon.coventry.gov.uk/directory_record/982/freedom_of_information_act_2000

7. Staff access to records and information

Only workers who have a legitimate need to access a person's record in their capacity as a Coventry City Council employee should do so. Staff should only access personal information as required by their job role and not for use in any other circumstances. Unauthorised access will lead to disciplinary action.

Personal information in every form should be kept securely so that people who are not authorised to view it do not have access to it. Records should be kept for a period in line with the Council's Retention and Destruction Schedule.

6. Information security

1. Storage of documents on computers and memory sticks

Personal information relating to service users or staff must not be stored on a computer desk top, c: drive or in ‘my documents’. The network folders (i.e. team or personal folder) must be used temporarily until transfer to Protocol ICS. These should than be deleted from shared drives.

Managers need to be aware of where staff store information and need to know the procedure for accessing that information in the event of that member of staff being absent from work.

Memory sticks (and other removable data storage devices) must be used with extreme care to stop Council information from being lost or disclosed.

Information that contains personal details or is labelled Protect or Restricted may only be stored on Council issued encrypted memory sticks.

Detailed guidance on using removable media/devices is in the Standard for the Management and Use of Removable Media Devices and is available on the Intranet at:
http://beacon.coventry.gov.uk

2. Working at home and taking information out of the office

Employees must ensure that information and equipment are kept securely. In particular, council information covered by the Data Protection Act must be kept secure at all times and must not be accessible to other household members.

Managers must be satisfied that all reasonable precautions are taken to maintain confidentiality of material in accordance with the requirements of the council's Data Protection and Information Security policies as outlined above.

Employees must discuss taking information covered by the Data Protection Act out of the office for work elsewhere with their manager.

3. Use of video, audio tapes, electronic and digital recording

These methods of recording should only be used when necessary, for example, when supporting communication with people with specific communication needs.

The use of video, audio and digital recording only takes place with the explicit consent of all parties.

The equipment used must be checked beforehand to ensure that it is designed for the specific purpose of recording multi-person meetings and that the quality is acceptable.

The explicit consent of a manager is required and the type of equipment, consents given and the reasons for use should be recorded in the record.

4. Reporting an Information Security Breach.

An information security breach is when information is accidentally or deliberately accessed, changed, or disclosed to someone who does not have a right to know it or it has been lost or destroyed in error.

Such breaches may cause real harm and distress to the individuals they affect lives may even be put at risk. For example, the harm caused by the loss or abuse of personal data (sometimes linked to identity fraud) include:

- Exposing addresses of vulnerable adults and children
- Confidential sources or witnesses being put at risk of physical harm or intimidation
- Fake benefit claims, credit card transactions etc
- The public and partner organisations losing confidence in how the Council handles their information
- The Council being fined up to £500,000 per breach

Information breaches involving personal data should be reported to the Information Governance Team on 024 7683 3323 or email infogov@coventry.gov.uk

Events or incidents involving ICT equipment or software problems should be reported to the ICT Service Desk on ex 7777 or email servicedesk@coventry.gov.uk

7. Records management

1. Retention of Records and Destruction of case files

No record should be deleted or destroyed without reference to the retention period for that record.

The Council's Retention and Disposal Schedule defines the minimum and permanent record retention periods for all records, transfer and archiving of records. The Schedule

- Identifies records that need to be retained permanently as part of the local archives;
- Prevents the premature disposal of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration;
- Provides consistency for disposing of records not required permanently;
- Provides consistent Records Management standards for the Council.

The Retention and Disposal Schedule is available on the intranet at: http://beacon.coventry.gov.uk