|  |  |
| --- | --- |
| New Logo 2 | |
|
| **Children’s Services Recording Policy and Procedure** | |
| **Sponsor:** | Corporate Director – Children’s Services Operations |
| **Owner:** | Assistant Director Data Protection and Data Governance |
| **Date Approved:** | 22/10/19 |
| **Date Reviewed:** | 11/05/21 |
| **Date of next review** | 11/05/24 |
| **Distribution:** | Non-Confidential, Internal and External Use |
|  | |
| 1. **Purpose** | |
| The purpose of this policy is to provide a framework for the recording of personal data about **service users**, **carers** and **supported lodgings providers,** and to identify where variation is permitted at service level, in order to promote good quality recording and to ensure that the statutory, regulatory, and contractual requirements are met.  The recording of personal data about **service users**, **carers** and **supported lodgings providers** is a critical part of service provision. It provides an account of the work undertaken for the benefit of the data subject, it may be used for reporting and quality assurance purposes, it provides a means of planning and evaluating the intervention and it may be used as evidence in case of a complaint, inquiry or other legal process. It must also be compliant with the requirements of The General Data Protection Regulation (GDPR), which means that it must be held securely, it must be accurate, it must be possible to identify where it is being stored and it must be deleted when it is no longer required for the purpose for which it was obtained. This policy and procedure enables these requirements to be met. | |
| 1. **Scope** | |
| This policy will apply to all personnel deployed by the two directorates, **Children’s** **Services Operations** and **Children’s Services Development and Innovation**.  This policy applies to the processing of personal data about service users, carers (including foster carers and adopters), supported lodgings providers and other third parties relating to work with these groups. It must be adhered to by all staff, volunteers, contractors, carers, students or agency workers recording personal data about these groups of people on behalf of Barnardo’s. It applies to data held electronically or as hard copy and includes audio and video recordings and photographs where the individuals are identified. Processing means everything that is done with the data including recording, storage, sharing, and deletion and archiving.  Personal data may be held as part of a case file or case recording, which is the written account of Barnardo's work with, or on behalf of, an individual, their family and/or carers. Personal data may also be held on databases and spreadsheets, in folders or other electronic or paper media and audio or visual recordings or photographs. It may be data that is being held temporarily, such as evidence of identity, or data that is held for a prolonged period of time or data that is to be archived. This policy includes data held on Barnardo’s IT systems as well as that processed by Barnardo’s staff, volunteers and carers using commissioners, partners or other third party systems. It does not cover the recording of personal data once it has been sent to Making Connection to be archived.  The policy includes requirements and procedures that are consistent with the current legislative requirements and policy developments in England, Scotland, Wales and Northern Ireland. Services that are subject to the requirements of regulatory bodies must comply with those requirements in addition to those contained in this policy and it is the responsibility of the ADCS and service manager to identify these and implement them within the service. | |
| 1. **Definitions and Key Concepts** | |
| **Data Processing:** This is anything that is done to or with personal data; it includes recording, storing, sharing and deleting.  **Data Protection Impact Assessment:** within the GDPR there is a requirement that an assessment is made of how we process personal data to ensure that it is compliant with the legislation and does not contravene the rights and freedoms of the people who data is being processed.  **Data Subject:** The data subject is the child, young person, adult, carer or supported lodgings provider who the recording is about.  **File Sign Off** is an audit of the file to ensure that the file contains all the necessary information and that the quality of the recording meets legislative and organisational standards and requirements.  **Closed Group**: This is a group with identified and consistent membership, usually operating for a defined period e.g. parenting group, activity group for disabled children, issue-based group for young carers. The members of the group would each have an individual case file.  **Open Group**: This is a group with a defined purpose which has a variable membership e.g. breakfast clubs, after-school clubs, and baby massage sessions. The members of the group may not have an individual case file.  **Personal data**: This is data which relates to a living individual who can be identified from the data.  **Service Recording Protocol**: This is a local protocol held by each service which identifies service requirements for recording where there is variance in the way that the policy may be implemented. This enables the service to be compliant with the regulatory, statutory and regulatory requirements that apply to it.  **Third party data**: This only refers to data in a record that is either about someone other than the subject of the record, which the subject has provided, or it is data about the subject provided by someone else.  **Third party confidential**: This only refers to data about the subject of the record provided by a third party which the subject is not aware of and the person providing the data has not given consent for it to be shared with the subject. | |
| 1. **Roles and Responsibilities** | |
| **ADCS or equivalents are** responsible for:   * Ensuring that operational managers are fully aware of their role and responsibility in relation to recording; * Quality assuring recording practice through sampling; * Driving improvements in recording practice.   **Management Information Officers** are responsible for:   * Providing staff with advice and support in relation to the recording of personal data; * Supporting managers to access and use the data recorded; * Providing support and advice to managers so that they can ensure that requirements of this policy are met.   **CSMs or equivalents** are responsible for:   * Ensuring that staff, carers, agency workers, contractors, students and volunteers are fully aware of their role and responsibility in relation to recording and that they implement the requirements identified in the Service Recording Protocol; * Quality assuring practice through sampling and case file sign offs; * Driving improvements in recording practice.     **Staff, carers, agency workers, contractors, students & Volunteers** are responsible for:   * Ensuring that recording is undertaken within the parameters of the Recording Policy & Procedure and the Service Recording Protocol. | |
| 1. **Policy** | |
| **Actions required before recording begins**   1. A **Data Protection Impact Assessment** must be completed and due diligence checks undertaken before recording of service user data by a new service begins or before a service starts to record data using a new system or starts processing data in a new way, such as using personal data for research purposes. 2. A **Service Recording Protocol** must be in place, using the standard template, for all services whether they record using Barnardo’s or third party systems. It must be reviewed annually or when there is a significant change in the data processing being undertaken. 3. Service user data must be recorded using electronic systems, hard copy must be scanned to the service user record. If there is a contractual or regulatory requirement to maintain data in hard copy the data must also be recorded on the electronic record and paper copies shredded when no longer required. This must be specified in the Service Recording Protocol. 4. The data subject must be informed that their data is being processed by Barnardo’s unless the party providing the data has informed the subject that it will be recorded by Barnardo’s, as in the case of third party referrals, or there is a legal basis which permits processing of data without informing the subject.   **Location, structure and content of recording**   1. Personal data relating to service users, carers and supported lodgings providers must only be stored in the designated locations, see Appendix 1, and must have an identified data subject and a retention date when closed. 2. Personal data that does not meet the criteria for a case file to be opened, see Appendix 1, must be saved in the Confidential Service User or Carer folder in Content Server. 3. Recording about server users accessing **open** or **closed** groups, see **Definitions and Key Concepts,** must be recorded as specified in Appendix 1. 4. Casework recording must follow the agreed structure of referral, assessment, plan, review and closure. The nature of the assessment and plan and the frequency of the reviews will be commensurate with the type of service delivered and level of risk being managed, must be agreed by the ADCS or equivalent and specified in the Service Recording Protocol. All cases must be reviewed at least annually, although it is expected that most cases will be reviewed on a more frequent basis. 5. Records should state the nature of contacts, e.g. visits, meetings, telephone calls, letters, e mails, texts etc. The record should contain a summary of the contact, including key issues and actions identified to address these issues. E mails or copies of other electronic communications must not be copied to the case record unless there is a specific reason to do so for evidentiary purposes. 6. Contacts must be recorded within five working days of the events or 24 hours if it concerns safeguarding. 7. Management decisions about a case that are taken in or outside supervision must be recorded in the case file within five working days of the decision being made or 24 hours if it concerns safeguarding. 8. The source of third party data about the subject of the record must be identified and the record should indicate if the subject is aware of the data and whether the third party has given consent for the data to be shared with the subject. 9. At the completion of the intervention a closure summary must be produced summarising what has been achieved and giving the reason for closure. 10. The appropriate retention date must be added to the case record before it is closed.   **Quality assurance and data quality**   1. Case files must be signed off by the line manager of the worker/s undertaking the recording. The frequency that the files are signed off will depend upon the nature of the work and the risk being managed; this will be identified in the Service Recording Protocol and will be approved by the ADCS. 2. All case files must be signed off unless the work is high volume and low risk, i.e. high numbers of cases with a small number of contacts that do not generally involve safeguarding, in which case the ADCS may agree that a percentage of case files may be signed off. At least 50% of the case files produced by each worker must be signed off in a 12 month period. This will be identified in the Service Recording Protocol. 3. Case files must be sampled by the ADCS and the CSM if they are not the line manager of the worker/s undertaking the recording. The number of case files that must be sampled will depend upon the nature of the work and the risk being managed, this will be identified in the Service Recording Protocol. At least one case file per worker per quarter must be sampled by the CSM and at least three case files per service per quarter by an ADCS. 4. The data in case files must be accurate and kept up to date.   **Recording Safeguarding concerns**   1. Safeguarding concerns about children, young people or adults at risk must be must be recorded within 24 hours. 2. If the subject of the concern does not have a case file, and they are a service user or the parent, child or sibling of a service user, a case file must be opened in the appropriate Barnardo’s or third party recording system. 3. If the concern relates to anyone else it must be recorded in Confidential Service User or Carer folder in Content Server.   **Management of paper and electronic records**   1. Closed paper records must be scanned to the electronic case file. 2. If there is no electronic case file the closed paper records must be archived, see (link to Corporate DP Policy), or catalogued, given a retention date and stored in a locked cabinet until the retention date is reached, when they should be securely shredded. 3. Closed electronic records must have a retention date added when closed, see (link to Corporate DP Policy) and records reaching that date must be sent for deletion.   **Data Protection**  25. Service user data must be kept secure at all times.  26. Data must only be printed out or removed from the service if an appropriate electronic version is not available, and there must be measures in place to ensure that it is always kept secure, which are documented in the **Service Recording Protocol.**  27. Personal data must be encrypted if sent by e mail, or sent in an envelope with the return address marked on the back, using special delivery if the letter contains personal data apart from personal descriptors.  28. Personal data must not be sent to or from staff or volunteer personal devices, unless there has been a risk assessment and this is approved by the ADCS.  29. Office equipment for disposal and premises being vacated must be thoroughly checked to ensure that no personal data has been left in them.  30. All subject access requests and information sharing requests must be recorded in the case file and the reasons for sharing or not sharing the data documented.  **Photographs and Video and Audio Recordings**  31.Photographs and audio and video recordings must be kept secure and only used for the purpose for which they were obtained.  32. Photographs and audio and video recordings must have a retention date and must be securely destroyed or deleted once this date is reached.  **Data Quality Procedure- For NHS Contracted Services only**  33.Services with an NHS contract or a requirement that they are compliant with the Data Protection and Security Toolkit must adhere to the procedures in Section 14 of the **Associated Legislation, Guidance, References and Documents**. | |
| 1. **Associated Legislation, Guidance, References and Documents** | |
| **Index**   |  |  |  | | --- | --- | --- | | **Section** | **Contents** | **Page Number** | | **1** | **Before the recording of personal data begins or before a new recording system or process is implemented** | **6** | | **2** | **Service Recording Protocol** | **8** | | **3** | **Location of saved personal data in relation to service users, carers or supported lodgings providers** | **8** | | **4** | **Informing data subject that their data is being processed** | **9** | | **5** | **Casework recording** | **10** | | **6** | **Recording third party data** | **14** | | **7** | **File Sign Off and Sampling of Case Files** | **14** | | **8** | **Recording Safeguarding Concerns** | **15** | | **9** | **Group work Recording** | **17** | | **10** | **Management of closed records** | **17** | | **11** | **Data Security** | **19** | | **12** | **Subject Access and Information Sharing Requests** | **22** | | **13** | **Photographs and Video and Audio Recordings** | **22** | | **14** | **Data Quality Procedure- For NHS Contracted Services** | **24** | |  |  |  |   **Please note** that when **staff** are referred to in this procedure it includes **as and** **when workers, agency workers, external consultants and students** who are processing personal data on behalf of Barnardo’s. Also where the term service user is used within a procedure it includes carers and supported lodgings providers**.**   1. **Before the recording of personal data begins or before a new recording system or process is implemented**    1. **Use of non-Barnardo’s system required by commissioner or partner**   **Action: BDU and/or Responsible ADCS or equivalent**   1. If a service is required to use a non-Barnardo’s system for service user recording, there must be a Data Protection Impact Assessment (DPIA) undertaken see (link to Data Protection Policy). 2. If a DPIA has previously been completed in relation to the required recording system this must be reviewed to ensure that it meets all of the requirements of recording; if not a new DPIA must be completed. 3. If the DPIA identifies risks that have not been adequately managed this must be discussed with the relevant Director and the DPO who are responsible for deciding whether the specified system may or may not be used by Barnardo’s. The DPIA is reviewed where risks are identified and plans are put in place to manage these. 4. The details of the system and how it will be used must be included in the Service Recording Protocol.    1. **Use of Barnardo’s systems**   **Action: BDU and/or Responsible ADCS or equivalent**   1. Review the DPIA for the specified system, including the Data Flows, and ensure that it meets the contractual or other requirements for the service. 2. If the DPIA identifies risks that cannot be adequately managed this must be discussed with the relevant Director and the DPO who are responsible for deciding whether the specified requirements may or may not be met by Barnardo’s 3. The details of the system and its use must be included in the Service Recording Protocol. 4. Identify any contractual requirements in relation to the processing of the data, including retention, responding to subject access and information sharing requests and management of data breaches. 5. If the commissioner or funder requires the deletion of service user records from Barnardo’s systems at the end of the contract discuss with them access to the records if there is a complaint or investigation in the future involving Barnardo’s staff or volunteers. Keep a record of any agreements. 6. If there is an agreement that the records will be deleted from Barnardo’s systems at the end of the contract consider implications that this may have for the way records are processed as part of the DPIA. 7. Identify any required actions to mitigate the risks identified and record these on the Service Recording Protocol**.**    1. **Implementing contractual requirements**   **Action: CSM**   1. Ensure that the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) includes the use of any external recording systems or any specific contractual requirements for the use of Barnardo’s systems; this should address which systems are to be used, what will be recorded on them and any arrangements for accessing external systems. Include which organisations will have access to service users’ information, the retention period of the data, where the data will be held when the contract has ended and how service users may access their records. 2. Ensure that all staff have read and understood the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) and are able to explain to service users where their information will be held and for how long, who will have access to it and how they can access their records. 3. Ensure that the [**Your Data Your Rights**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329106825/21352_Your_Data_Your_Right_Leaflet_v3.pdf?func=doc.Fetch&nodeid=329106825) or the[**Welsh Translation**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329105821/21352_Your_Data_Your_Right_Leaflet_WELSH_Translation.pdf?func=doc.Fetch&nodeid=329105821) includes the relevant information about the use of non-Barnardo’s systems or specific contractual requirements if using Barnardo’ssystems. 4. **Service Recording Protocol**    1. **Producing and reviewing the Service Recording Protocol**     **Action: Children's Services Manager**   1. Produce a[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)for all services using the standard Proforma and pass to the ADCS for approval. 2. Review the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)at least annually and pass to the ADCS for approval. 3. Update the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)whenever there is a change in the service recording procedures and/or requirements. 4. Store the revised protocol in the Service Information folder in Content Server. 5. Ensure all staff and volunteers are informed of any revisions to the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.**   **Action: ADCS or equivalent** 1. Approve the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)and sign off the reviewed document on an annual basis.   1. **Location of saved personal data in relation to service users, carers or supported lodgings providers**    1. **Storage of personal data**   **Action: CSM**   1. Ensure that personal data is only saved in a designated location, see chart in Appendix 1. 2. Personal data is subject to all of the requirements of GDPR no matter where it is stored or if it is stored electronically, as hard copy or a video or audio recording; ensure that the data subject is identifiable, there is a retention date and the data is deleted when that date is reached or the service is closed. If the data needs to be retained after the service is closed discuss arrangements for the management of this with the ADCS.    1. **Recording personal data in a confidential area in content server document management**   **Action: CSM**   * 1. Ensure that an area called Service User Confidential or Carer Confidential is set up in the appropriate confidential area of content server document management.   2. Ensure that permissions to access the confidential area are restricted to those who have a right to access any of the data contained within it.   3. Inform staff who have permissions to access the Service User/Carer Confidential area that they must only access documents which they have a right to see and that accessing the documents if they do not have the right to do so could result in disciplinary action.   4. Ensure that folders are created within this area to hold the personal data. The actual folder structure may be determined by the service or Regional, National, Business Line office, but it must be documented in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)and staff understand that they must save the data in the correct folders.  1. Ensure that a sub folder is created for each individual or spreadsheet or activity. 2. Ensure that the following naming convention for the sub folder containing the personal data must always be used,  * First name and surname of service user or carer/ retention date e.g*. Grace Smith 29 10 18* * Name of spreadsheet/ retention date e.g. *Future Matters Quarterly Reporting to MCC Deletion 3 months after reporting* * Name of activity/ retention date e.g. *DP Breach* Investigation 12 10 19.  1. Ensure that the Service User/Carer Confidential folder is reviewed at least quarterly and subfolders that have reached the retention date are deleted. 2. Ensure that the data held in the ServiceUser/Carer Confidential folder is included in the data search whenever there is a subject access request or information sharing request. 3. Ensure that all staff are aware of the Service User/Carer Confidential folder and the procedure for the naming and use of the sub folders.   **Action: All staff**   * 1. Record personal service user and carer data that meets the criteria set out in this section in the Service User/Carer Confidential folder.   2. When recording data in the Service User Carer Confidential folder set up a sub folder for each individual, spreadsheet or activity using the following naming convention * First name and surname of service user carer/ retention date e.g*. Grace Smith 29 10 18* * Name of spreadsheet/ retention date e.g. *Future Matters Quarterly Reporting to MCC Deletion 3 months after reporting* * Name of activity/ retention date e.g. *DP Breach* Investigation 12 10 19.   1. If the retention date has changed during the period of time that recording has occurred in the sub folder, ensure that the name of the sub folder is updated to accurately reflect the period for which the data must be retained.  1. **Informing data subject that their data is being processed**   **4.1 Informing service user/carer/supported lodgings providers** **that a record will be held about them**  **Action: All staff**   1. Service users, carers and supported lodgings providers must be given a copy of[**Your Data Your Rights**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329106825/21352_Your_Data_Your_Right_Leaflet_v3.pdf?func=doc.Fetch&nodeid=329106825) or the[**Welsh Translation**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329105821/21352_Your_Data_Your_Right_Leaflet_WELSH_Translation.pdf?func=doc.Fetch&nodeid=329105821),at the beginning of their involvement with Barnardo’s and this must be recorded on the case file. This may be done using the appropriate field on core data or as a case note entry. This may be done in person or it may be sent by post or email. 2. Discuss the content of the document with the service user and record this discussion in the case file. 3. If the record is held on the commissioner’s system and they are the Data Controller ensure that a copy of their privacy notice is given to the service user. 4. If the service user is too young to understand theinformation being given, a parent or person with legal responsibility must be informed on their behalf. This must be reviewed at least annually and when the service user is old enough they must be given the information in an understandable format. 5. If the service user does not have the mental capacity to understand the information being given, a parent or person with legal responsibility must be informed on their behalf. If there is no-one with legal responsibility a best interests assessment must be undertaken and recorded on the case file, see[**Mental Capacity Act and DoLS Policy.docx**](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=251075284)**.**   **Action: Responsible Manager**   * 1. Ensure that service users are being given the privacy notice and Your Data, Your Rights leaflet at the start of the intervention as part of quarterly monitoring of core data forms and ensure that staff are recording that they have fully explained what information about service users is shared or recorded.   **4.2 Informing service users who do not have a case file that their data will be recorded**  **Action: CSM**   * + 1. Identify if any personal data is being recorded about service users outside a case file. This may include attendance lists.     2. Inform the subject that their data is being processed through the provision of Your Data Your Rights if possible.     3. Where it is not possible to provide a copy of Your Data Your Rights in person inform them verbally, and record this, or ensure that there is a written statement, on signing in forms or referral forms for example, of what data will be recorded, for what purpose and what will happen to it.     4. If data is being held on an online system accessed by the data subjects ensure that there is a Privacy Notice on that system that explains what data will be recorded, for what purpose and what will happen to it and their rights in relation to that data.  1. **Casework recording**    1. **Opening or re-opening a case file**   **Action: CSM**   * 1. Ensure that the process for opening or re-opening case files is documented in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)including who is responsible for deciding to re-open the case file and who is responsible for actioning it.   **Action: Responsible Worker**   1. If re-opening a case file ensure that the data held about the service user, including contact and profile data, is up to date and amend any incorrect data.    1. **Structure of casework recording**   **Action: All staff and volunteers recording personal data**   * + 1. All casework recording must be based on the structure of; * **Referral**- identifying and contact details and reason service requested * **Assessment**-identification of needs and whether these can be met by service * **Plan**-identification of actions to meet needs, who will do them and timescales * **Review**- consideration of progress made and identification of further actions required * **Closure summary** including what has been achieved, information about safeguarding issues and reason for case closure.  1. In addition the case record will include any risk assessments undertaken in respect of the subject of the record, a record of contacts with or about the service user, carer or supported lodgings provider or the others associated with them. This will include personal data shared by third parties about the service user, carer or supported lodgings provider. 2. The form of the referral, assessment, plan, review and closure will vary according to the nature of the work being delivered and the contractual, statutory or regulatory requirements. 3. In high volume low intensity cases, where there may be only one or two contacts, one or more elements may be covered in one contact or in low volume high intensity work one or elements may take several contacts to complete. The requirements for each service, including the forms to be used, must be agreed by the ADCS or equivalent and included in the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader). 4. A referral may be a self-referral, made by the subject of the file themselves, or made on their behalf by a third party such as another agency or a relative. It should include at least the name, contact details, date of birth of the subject and the reason that the service is being requested. 5. The assessment should include an identification of the needs of the subject to enable a decision to be made of whether to offer a service. 6. The plan should be based on the assessment, as well as the contractual, statutory and regulatory requirements, and should set out the aims of the intervention and how these will be achieved. 7. There should be a review of the plan at a frequency appropriate to the intervention; this would include a record of progress and any changes to the original plan. 8. At the end of the intervention a closure summary must be produced by the caseworker which identifies what has been achieved, the reason for closure and any critical information in case the case is re-opened in the future, such as safeguarding concerns. 9. A retention date must be added to the record at closure, this should be identified with reference to  [The Retention Archiving and Deletion of Records Policy](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=259569564). 10. The subject of the record, or where appropriate their parent or carer, must be involved in all parts of the process and their views recorded. If the subject does not have the mental capacity to make decisions on their own behalf the [Mental Capacity Act and DoLS Policy](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=251075284) must be followed.     1. **Recording contacts**   **Action: All staff and volunteers recording personal data**   1. Record all contacts as soon as possible after the event has taken place and within a maximum five working days of the contact having taken place or within 24 hours if it relates to safeguarding. 2. Enter an individual record for each separate contact. If multiple attempts are made to contact someone on one day these may be entered as a single contact. 3. Name the contact recording using the naming convention agreed for the service and set out in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.** 4. Apply the appropriate documents classification to the recording if this is required for the recording system being used. Those required by a service should berecorded in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.** 5. Ensure that all of the relevant areas below are addressed in each contact recording:  * Separate observed or verified facts from opinions and ensure that opinions are clearly identified as such   + Indicate professional assessment/judgment   + Record significant events in the service user’s life   + Record the service user’s experiences from his/her perspective and include their views and opinions of what has happened or is being planned   + Use only non-judgmental and non-discriminatory language   + Ensure that the recording is accurate, ethical and relevant   + Reflect Barnardo’s Basis and Values, legislative requirements and equalities issues   + Demonstrate how the contact has contributed to achieving the plan and outcomes where applicable   + Record agreed actions or work to be undertaken with identified timescales.  1. Telephone calls, e mails and contact from other sources, such as texts or social media, must be recorded in contacts. The source of the contact, the type of contact and a summary of the content must be recorded in the case file. All or parts of E mails must not be copied to the case file, unless required for evidentiary purposes which would require the production of the original e mail. 2. Letters must be scanned onto the case file.    1. **Recording an assessment, plan or review or other personal data received from another agency**   **Action: Responsible Worker/Administrator**   1. If the data is in an electronic format save to the case record including the name, role and agency of the person providing the data. If possible record whether the person providing the data consents to it being shared with the data subject. When naming the contact identify the type of document, e.g. review. 2. If the data is in a paper format scan to the case record including the name, role and agency of the person providing the data. If possible record whether the person providing the data consents to it being shared with the data subject. When naming the contact identify the type of document e.g. Review.    1. **Outcomes/Impact**   **Action: CSM**   * + 1. Identify the system that is to be used to measure and report on outcomes in the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader), including instructions for recording these on the case file.     2. Ensure that staff understand how to measure and record outcomes using the agreed system and ensure that they are implementing this.     3. If it is not possible to measure outcomes in relation to each individual, for instance if the intervention is very short and it is not possible to have a minimum of two assessments, an alternative way of measuring impact should be agreed with the ADCS and recorded in the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader).   1. **File Closure**   **Action: CSM**   1. Identify the minimum period without any contact after which file closure must be considered and record in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.**     **Action: Responsible Worker**   1. Agree with the line manager that the case may be closed. 2. Check that the core data is up to date and amend any incorrect data. 3. Complete a closure summary which identifies what has been achieved the reason for closure and any critical information in case the case is re-opened in the future, such as safeguarding concerns. 4. If the recording system used includes classification of documents classify as case closure. 5. Note if there are any corresponding paper records/externally held records in relation to the file. 6. Add the appropriate retention date to the record; see the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.** 7. If there is an existing retention date, review and amend this if necessary. The latest retention date must always be the latest applicable date*.*     **Action: Line Manager**   1. If the file has not been signed off previously, undertake a file sign off following the procedure stated in Section 7. 2. Ensure that the closing summary and outcomes assessments have been completed satisfactorily. 3. Ensure that the correct retention period has been added to the core data form. 4. Close the intervention or the case file in line with procedure applicable to the recording system being used.    1. **Recording management decisions including decisions made in supervision**   **Action: CSM and line manager**   1. Identify who is responsible for recording management decisions including decisions made in supervision and record this in the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader). 2. Ensure that these decisions are being appropriately recorded when signing off or sampling service user records. 3. Ensure that if the person who would usually record the management decision is not available the decision is recorded by another who has knowledge of the decision being made and has responsibility for its implementation.   **Action: Individual responsible for recording management decisions**   * + 1. Record the management decision or decision made in supervision on the case file as soon as possible after the decision has been made; this must be within 5 working days of the decision being made and within 24 hours if it involves safeguarding.     2. Record the name and job title of the manager making the decision, the reason for the decision, details of the action required and timescales for the action to be implemented.     3. Record when the action/s have been completed as well as any issues that prevented the actions being achieved.  1. **Recording third party data**    1. **Recording third party information**   **Action: Responsible Worker**   * 1. Record information about a third party provided by the subject in the case file or record, identifying that it was the subject who provided the data. The third party does not need to be informed directly that their data is being recorded as this is covered by the Barnardo’s Privacy Notice on the website.   2. Record data provided by a third party about the subject on the case file or record, identifying the name and role of the person who provided it.   3. Identify if the third party has consented to the data being shared with the subject if they are not already aware of it. It is good practice for the subject to have access to as much of their data as possible and efforts to obtain consent to share should be made unless this could cause harm to the subject or the individual providing the data.   4. Identify the data as “third party confidential” if there is a process for doing this, such as tagging the recording or use of a folder, only if the subject is unaware of the data and the third party has not given consent for it to be shared with them. Please note that identifying data as third party confidential does not mean that it will not be shared with the data subject if they make a subject access request. The third party, or their agency, must provide a legal basis for the data not being shared; see (Link to Corporate DP Policy).  1. **File Sign Off and Sampling of Case Files**    1. **Setting the frequency of case file sign off**   **Action: ADCS or equivalent**   * 1. Agree with the CSM the frequency that case files must be signed off by the line manager. The frequency should reflect the levels of risk associated with the work and the resultant level of oversight required from the manager, and the intensity and frequency of the involvement with the service users. The minimum frequency for file sign off should be once every 12months.   2. In the case of services undertaking low intensity work with a very high volume of service users and where the risks being managed are low; a percentage of case files to be signed off annually may be agreed by the ADCS/AHoB. At least 50% of the case files produced by each worker must be signed off in a 12 month period. This will be identified in the Service Recording Protocol.   3. All cases involving safeguarding or other areas of concern or identified risk must be signed off by the line manager.   **Action: Children’s Services Manager**   * + 1. Agree the frequency of case file sign off with the ADCS and record in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) and ensure that the managers responsible for case sign off understand what is required.     2. Ensure that all cases involving safeguarding or other areas of concern or identified risk are signed off by the line manager.   1. **Signing off SUR case files**   **Action: Responsible Manager (Team Leader or above)**   1. Sign off all, or the designated percentage, of the case files within a service or team at the required frequency, as stated in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.** 2. Read all of the data recorded since the last file sign off undertaken by the responsible manager (or from when the case file was opened if this is the first file sign off). 3. Record the file sign off using the[**FILE SIGN OFF PROFORMA**](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=244232413)and save in the service user record. 4. Address any issues with the quality of recording/staff performance with the staff member concerned and record them in the supervision notes or make a file note in the staff file. 5. If the case file has not been signed off during the intervention sign off the case file at case closure.    1. **Sampling SUR case files**   **Action: CSM if not the responsible first line manager**   1. Sample the number of case files designated in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader), this must be a minimum of five case files per quarter per service and should include recording by different members of staff. 2. Read all of the data covering a minimum period of six months (or from when the case file was opened if this was less than six months). 3. Record the sampling using the[**File Sign Off Pro-Forma**](http://intranet/Interact/Pages/Content/Document.aspx?id=8600&SearchId=)and save in the case file. 4. Address any issues about the quality of recording with the line manager and/or the staff member concerned and record these through supervision.   **Action: ADCS or equivalent**   1. Sample the number of case files designated in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader), this must a minimum of three case files per service per quarter and should include recording by different members of staff. 2. Read all information in the case file covering a minimum period of six months (or from when the case file was opened if this was less than six months). 3. Record the file sampling on the case[**File Sign Off Pro-Forma**](http://intranet/Interact/Pages/Content/Document.aspx?id=8600&SearchId=)and save in the case file. 4. Address any issues concerning the quality of recording with the CSM and record this in the supervision record.    1. **File sign off and sampling records stored on non-Barnardo’s systems.**   **Action: CSM**   * 1. Agree with the commissioner how case files will be signed off and sampled.   2. Record the agreed process in the [Service Recording Protocol](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader).  1. **Recording Safeguarding Concerns**   **8.1 Recording a safeguarding concern about a child/young person under the age of 18 years or an adult at risk.**  **Action: All staff**   1. Record any safeguarding concerns within 24 hours of the concern being identified in accordance with the Barnardo's Corporate Safeguarding and Protecting Children Policy and Procedures or The Corporate Safeguarding Adults at Risk policy and follow the correct procedure for responding to a concern. 2. If the Safeguarding status of the child or young person is identified on the case file changes, enter or update the information on the case file.   **Action: All staff or volunteers without access to service user file**   1. Record any safeguarding concerns within 24 hours of the concern being identified in accordance with Barnardo's Corporate Safeguarding and Protecting Children Policy and Procedures or Corporate Safeguarding Adults at Risk policy and follow the correct procedure for responding to a concern. 2. The document must be clearly titled and, dated and signed. 3. Pass to the responsible manager for the service immediately or the covering manager if they are not available, identifying as a safeguarding concern.   **Action: Responsible Manager**   1. Ensure that the Barnardo's Corporate Safeguarding and Protecting Children or Corporate Safeguarding Adults at Risk Policy and Procedures have been followed. 2. If the person with the concern doesn’t have access to service SUR file room, identify who is responsible for scanning and saving the recording or typing up and saving the contact recording. 3. If the concern is about a child/young person or adult at risk who has a closed case file, the decision to reopen the case file will be made depending on the level of action/on-going contact with/about the child/young person. 4. Ensure that all decisions and actions identified/taken as a result of the concern are recorded accordingly.   **8.2 Recording a concern/safeguarding concern about a child/young person or adult at risk where there is no case file**  **Action: Responsible manager or worker**   * 1. If the subject of the concern is a service user or a parent, child or sibling of a service user open a case file in the electronic case recording system used by the service.   2. Inform the subject of the record or their parent that a record has been opened about them and give them a copy of [**Your Data Your Rights**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329106825/21352_Your_Data_Your_Right_Leaflet_v3.pdf?func=doc.Fetch&nodeid=329106825) or the[**Welsh Translation**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329105821/21352_Your_Data_Your_Right_Leaflet_WELSH_Translation.pdf?func=doc.Fetch&nodeid=329105821).   3. If the subject is not a service user or a parent, child or sibling record the concerns in a folder in Service User /Carer Confidential folder in the appropriate confidential area of content server document management. The folder must have the name of the subject and a retention date. If it is a Serious Safeguarding matter report using the process set out in the Barnardo's Corporate Safeguarding and Protecting Children or Corporate Safeguarding Adults at Risk Policy and Procedures   4. Record the safeguarding concerns within 24 hours of the concern being identified in accordance with Barnardo's Corporate Safeguarding and Protecting Children or Corporate Adults at Risk Policy and Procedure and follow the correct procedure for responding to a concern.  1. **Group work Recording**     1. **Recording when service users attend a closed group, i.e. groups where all of the members have an individual case file.**     **Action: Responsible Worker**   1. Identify individual case files and link them to the group. 2. Enter recording for each group session and copy to case file of all group members attending group ensuring that recording copied does not contain any personal data in relation to individual group members.    1. **Recording when service users attend an open group i.e. groups where all of the members do not have an individual case file.**     **Action: Responsible Worker**   1. Ensure that a folder for the group has been set up in the Service User /Carer Confidential folder in the confidential area of content server document management. 2. The name of the folder must include the name of the group and the retention period, which is 6 years from the closure of the group. 3. Where there is a variable programme, you must record the activity for each session. Where the activity is constant e.g. a breakfast club, there does not need to be an entry each time the group is held. 4. If there are any safeguarding concerns, you must open an individual case file for the individual concerned, in whichever recording system is being used for service user or carer data. 5. If personal data about the individual members of the group are recorded, including their name, they must be given a copy of the privacy notice and Your Data, Your Rights leaflet which explains what is recorded about people attending the group and the retention period.    1. **Recording of sessions run by Barnardo's staff on behalf of, or with, other agencies**   **Action: Children's Services Manager**   1. Ensure the Service Recording Protocol stipulates the procedure for complying with Data Protection Act requirements and for capturing necessary monitoring data. 2. Ensure that there is a written agreement with the other agency/ies regarding the collation of relevant data, recording and the relevant policies and procedures that will be followed including safeguarding, health and safety, and complaints/representations. 3. Ensure that all staff/volunteers delivering the session have read and understand the above agreement. 4. **Management of closed records**   **10.1 Management of paper records**  **Action: CSM**   * 1. Identify if there is a contractual or regulatory requirement to maintain a paper record and record this in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader). If there is no such requirement all paper records must be scanned to the case file and the paper copy securely shredded.   2. Identify a lockable filing cabinet in a secure area in which the paper files are to be stored.   3. Ensure that a signing out system is set up so that if a paper record is removed from the cabinet there is an audit trail showing who removed the record, the date that it was removed and the date returned and who returned it.   4. Ensure that a Record of Paper Files is maintained in Service User /Carer Confidential, which includes the case ID number and the service user name. If the paper record contains information not contained in the electronic record ensure that the content of the paper record is read as part of the file sign off.   5. Ensure that when electronic files are sent for deletion the corresponding paper file is shredded.   6. Ensure that any paper files that require archivingare sent to Making Connections.  1. Ensure that at least annually any paper files are audited to ensure that all records are accounted for and a record of this is maintained. 2. If any record cannot be located this is a potential breach of the Data Protection Act and the (link to Corporate DO Policy)policy on reporting Data Breaches must be followed. 3. Ensure that any other paper records containing personal data, such as day books or records of medication, are stored securely with access only by authorised persons. These must be securely destroyed when the retention date is reached, see Corporate Data Protection Policy. 4. If the service stores historical paper records due to the deletion date not yet being reached and there being no equivalent electronic case file, ensure that a list of these is maintained including name, date of birth, retention date and date when record has been shredded. 5. Undertake an annual audit of paper records to ensure that they are safe. 6. Every quarter securely shred paper records which have reached their deletion date.   **Action: All staff and volunteers**   1. All service user paper records must be scanned onto the electronic service user record unless they are part of a group record such as a day book. 2. Where there is a contractual or regulatory reason to maintain a paper record in addition to the electronic, securely shred the paper record when this is no longer required, as stated in the Service Recording Protocol. 3. When removing a paper file from the filing cabinet ensure that the date it is removed, the date it is returned and your name is recorded on the record tracking system.   **10.2 Identifying the retention period for electronic case files**  **Action: Responsible Manager/CSM**   1. Identify the correct retention period for the case file using[(Link to corporate DP Policy)**.**](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=259569564) 2. Specify the relevant retention periods for the service in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.** 3. Ensure that the correct retention date has been entered onto the case file when the case is closed.   **Action: Responsible worker**   1. Enter the retention date onto the case file when the case is due for closure. 2. If there is an existing retention date the case file must be retained for whichever date is the longest; enter this date onto the case file.   **10.3 Action required when electronic case files have reached the retention date**  **Action: CSM**   1. Every quarter run the case report identifying cases that have reached the retention date. 2. Check the report to ensure that there are no apparent errors. 3. Send the list of cases for deletion to [surdeletion@barnardos.org.uk](mailto:surdeletion@barnardos.org.uk) or equivalent if not using Content Server SUR. 4. Check if there are any paper records for subjects of case files due for deletion. 5. Arrange for the paper records to be securely shredded.    1. **Action when a service recording on Barnardo’s systems closes**     **Action: CSM**   1. Ensure that all case files have been closed. 2. Ensure that all case files have a retention date added. 3. Ensure that all files that have reached the retention date have been sent for deletion. 4. If recording on content server SUR confirm to the ADCS or equivalent and the Content Server Team that the file room is ready for closure. 5. Complete the fields on the Service Information Form identifying where the records relating to the service are stored.   **Action: ADCS or equivalent**   * + - 1. Ensure that all of the requirements in relation to the closure of the service records have been met.   1. **Action when a service recording on a non-Barnardo’s systems closes**   **Action: Service Manager**   1. If all of the service user data is held on a non-Barnardo’s recording system ensure that any management information to be retained has been collected and saved. 2. If there is data on Barnardo’s systems that needs to be returned to the commissioner ensure that has been done.   **Action: ADCS or equivalent**   * + - 1. Ensure that all of the contractual requirements in relation to the transfer or disposal of service records have been met.  1. **Security of personal data**    1. **Printing of personal data from electronic record**   **Action: CSM**   1. Identify whether it is necessary for the delivery of the service for personal data to be printed off from the electronic record. 2. State in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)the circumstances in which information may be printed off from the electronic record. 3. Ensure that staff understand that they must only print off information from the electronic record for a purpose identified in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) or with specific permission from their line manager. 4. Ensure that staff understand that they must keep paper copies of records secure at all times and must destroy these when the purpose it was produced for has been met. 5. Ensure that staff know that if copies of personal data are being produced for a meeting they must ensure that these are retrieved at the end of the meeting. If participants in a meeting are permitted to take copies of personal data ensure that these are watermarked as “Distributed” and there is a written agreement with those third parties about what they may do with the data and the requirement that it is kept secure.   **Action: All staff/volunteers with access to service user recording**   1. Read the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) and only print off records from electronic systems for the purpose specified within this. 2. If there is a need to print off records for any purpose not specified in the [**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader), seek permission from a line manager and only print off the information if this is given. 3. Keep all hard copies of information secure and destroy as soon as the purpose it was produced for has been met. 4. If copies of personal data are distributed to third parties who may retain these ensure that the documents have a “Distributed” watermark.    1. **Removing personal data from the service**   **Action: Service Manager**   1. Identify if there is a need for documents containing personal data to be held outside the service:, this will include documents to be taken to meetings, notes of meetings, manual recording, copies of information required by staff, carers and volunteers operating in the community, records held by staff who are home based. 2. Identify if there is any special equipment required to keep this information secure, such as filing cabinets, lockable boxes, and ensure that this is provided. 3. Ensure that staff and volunteers understand the precautions that must be taken to keep documents secure when they are removed from the office. 4. Record the circumstances when documents may be held outside the office and the precautions that must be taken to keep them secure, in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader)**.**   **Action: All staff and volunteers**   1. Do not remove documents containing personal data from the office, or keep these at home unless this has been agreed by the line manager and documented in the[**Service Recording Protocol**](https://livelink.barnardos.org.uk/otcs/llisapi.dll?func=ll&objId=309806050&objAction=viewheader) or specific consent has been given by a line manager. 2. Documents kept at home must be stored in a locked drawer or cabinet when not in use and must not be accessed by anyone who does not have a right to view them. When no longer required they must be shredded using a cross cut shredder or returned to the office. 3. Documents taken outside the office or home must not be left unattended, for example they must not be left in a car boot. 4. When transporting documents make sure that they are secure, e.g. use an opaque folder and carry them in a bag with a cross body strap or ruck sack if you need to be hands free. 5. Pages with notes containing personal information should be removed from notepads/books upon returning to the office, and stored in a locked drawer or cabinet until they have been entered onto the electronic record and then securely shredded. If there is a reason to retain a paper record this must be stored in an individual service user record for as long as it is required.    1. **Sending personal data outside the service**   **Action: All Staff**   * 1. Encryption protects the e mails sent to mailboxes outside of Barnardo’s while in transit. Encryption must be used when sending personal data to recipients outside Barnardo’s unless required by the commissioner to use another system to safeguard e mails in transit, such as Egress.   2. Always use the blind copy facility (bcc) when sending an e mail to a group of recipients and you are using their personal email addresses. If this is not done the whole group will have access to everyone’s personal e mail address which is a data breach.   3. Regularly review e mail contacts list and delete any that are not needed. A number of emails are sent to the incorrect recipient because the wrong name is selected from the list of names automatically generated by the contacts list.   4. If an email is sent to the incorrect recipient inside Barnardo’s recall the e mail. Please note that if the e mail address is outside Barnardo’s the recall function does not work.   5. Letters that contain personal data must have a return address and contact phone number on the outside of the envelope. If including the name of the service could give information about the recipient, e.g. Domestic Abuse Team, this should be omitted.   6. Decide what level of security is needed when sending personal data by post depending upon the content of the mail. For example; if it is an invitation to an appointment ordinary mail may be sufficient but if it contains reports or documents belonging to the recipient, special delivery should be used.   7. If the case files are being sent as hard copy a courier service must be used unless these are delivered in person, in which case a receipt of delivery must be obtained.   8. **Disposal of office equipment and clearing of premises**   **Action: CSM**   * + 1. Ensure that any office equipment used for storage of personal data has been thoroughly checked to ensure that all such data has been removed before it is disposed of.  1. Ensure that the person checking the equipment has completed the [Disposal of Office Equipment Sign Off Form](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=295271252). 2. When satisfied that there is no personal data remaining in the equipment sign the [Disposal of Office Equipment Sign Off Form](http://livelink.barnardos.org.uk/otcs/llisapi.dll?func=doc.ViewDoc&nodeid=295271252) to authorise disposal. 3. Save the completed form to the Service Information folder and update the service inventory if applicable. 4. Ensure that all personal data has been removed from premises that are no longer to be used before the premises are vacated. 5. **Subject Access and Information Sharing Requests**    1. **Responding to a request to access a file by a service user**   **Action: All staff and volunteers**   * 1. If a service user, carer or supported lodgings provider has made a verbal request for a copy of their record or requests this in writing inform the CSM immediately.   2. Inform the person making the request that the CSM will be informed and their request will be responded to.   **Action: CSM**   1. Follow the procedure in (link to Corporate DP Policy). 2. Ensure that all requests are recorded on the case file. 3. If there is no case file record the requests in a folder in Service User/Carer Confidential folder Content Server document manager.    1. **Photographs and Video and Audio Recordings**    2. **Recording photographs and video and audio recordings**   **Action: Service managers, team leaders, practitioners and volunteers**   1. Photographic and video images of people and audio recording are personal data and are subject to the requirements of the General Data Protection Regulation. 2. Ensure that staff and volunteers understand that only Barnardo’s cameras or recording equipment may be used to take photographs or make recordings of service users; personal devices must not be used. 3. If photographs or audio or video recording are used as part of the work of the service include this in the [**Your Data Your Rights**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329106825/21352_Your_Data_Your_Right_Leaflet_v3.pdf?func=doc.Fetch&nodeid=329106825) or the[**Welsh Translation**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329105821/21352_Your_Data_Your_Right_Leaflet_WELSH_Translation.pdf?func=doc.Fetch&nodeid=329105821)**.**   **Action: All staff**   1. Only use Barnardo’s cameras or recording equipment to take photographs or make recordings of service users; personal devices must not be used. 2. If the use of photographs, video or audio recording is not included in the [**Your Data Your Rights**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329106825/21352_Your_Data_Your_Right_Leaflet_v3.pdf?func=doc.Fetch&nodeid=329106825) or the[**Welsh Translation**](https://livelink.barnardos.org.uk/otcs/llisapi.dll/329105821/21352_Your_Data_Your_Right_Leaflet_WELSH_Translation.pdf?func=doc.Fetch&nodeid=329105821)obtain consent using   [**Consent for photographs video or audio recording form**](http://livelink.barnardos.org.uk/livelink91/llisapi.dll?func=doc.ViewDoc&nodeid=295267896)**.**   1. If subject access requests are received these may include photographic and video images or audio recordings. Check if the service holds this type of data and identify any such data held on the subject of the request. 2. Review all photographs within five working days after they have been taken and only retain the images required for the purpose for which they have been taken retained. Delete all surplus images.    1. **Storage and Management of Photographs**     **Action: Service managers, team leaders, practitioners and volunteers**   1. Save photographs to the case file within 5 working days and delete from the memory card. 2. If there is no case file save the photographs to a folder in Service User/Carer Confidential. Ensure that the folder has a retention date. 3. Store the memory card in a locked cabinet or safe until all the images have been downloaded, printed or deleted. 4. If photographs are to be printed off for use, such as for learning logs, print these off and ensure that the digital image is deleted unless it is required for another purpose. 5. Store photographs that are printed off securely in a locked cabinet in a file or folder which identifies the subject/s of the photograph and the retention period. A process to track photographs that are removed from the cabinet must be in place. 6. Store photographic images that are not saved to the individual service user or group file or printed on encrypted memory sticks only. The encrypted memory stick must be stored in a locked cabinet or safe when not in use. 7. Catalogue the images stored on each memory stick with the name/s of the subjects of the photographs, the purpose for which the images are being held and the retention date. Store a copy of this with the encrypted memory stick and the consent forms. 8. Delete photographic images from the memory stick device when the retention date is reached. 9. When the service closes ensure that all photographs held on encrypted devices are deleted unless they are to be shared with the commissioner or new provider or there is any other specific reason for them to be retained. If the images are retained a manager must be identified to assume responsibility for the security of the images and to ensure that they are deleted when the retention date is reached. 10. Ensure that any images to be retained by Barnardo’s after the closure of the service are saved to an encrypted memory stick. Catalogue the images stored on each memory stick with the name/s of the subjects of the photographs, the purpose for which the images are being held and the retention date. Store a copy of this with the encrypted memory stick and the consent forms.   **Action: ADCS or equivalent**   * + 1. Ensure that if any images are retained on encrypted devices after the closure of a service they are stored in a secure place and are deleted once the date has been reached.   1. **Storage and Management of Video and Audio Recordings**   **Action: Service managers, team leaders, practitioners and volunteers**   1. Store video and audio devices containing service user images or audio recordings in a locked cabinet or safe when not in use. A tracking system must be in place to identify when storage devices are removed from the cabinet and by whom and when they are returned. 2. Review video and audio recordings within five working days after they have been made and only retain the recordings required for the purpose for which they have been made. Delete all surplus recordings and delete any that are not required. 3. Save video and audio recordings that are to be recorded as part of the work with an individual or a closed group to the case file or group file within five working days and delete from the recording device. 4. Save any video and audio recordings that are not required to be recorded on the individual or group file to an encrypted memory stick within five working days and delete from the video or audio device. 5. The video or audio recordings stored on each memory stick must be catalogued with the name/s of the subjects, the purpose for which the images are being held and the retention date. They must be deleted when the retention date is reached. Consent forms must either be stored with the memory stick or the catalogue state where these are held. 6. If the files generated by video recordings are too large to be stored on individual case or group files store these on encrypted memory sticks and cross reference them to the case or group file. 7. When the service closes ensure that all video and audio recordings held on encrypted devices are deleted unless they are to be shared with the commissioner or new provider, or there is any other specific reason for them to be retained. If the recordings are retained a manager must be identified to assume responsibility for the security of the recordings and to ensure that they are deleted when the retention date is reached. 8. Ensure that any recordings to be retained by Barnardo’s after the closure of the service are saved to encrypted memory sticks. Catalogue the recordings stored on each memory stick with the name/s of the subjects of the recordings, the purpose for which the recordings are being held and the retention date. Store a copy of this with the encrypted memory stick and the consent forms. 9. **Data Quality Procedure- For NHS Contracted Services**   Please note that this procedure applies to services with an NHS contract or a requirement that they adhere to the Data Protection and Security Toolkit.   1. **Purpose**    1. The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation.       1. Procedures for ensuring data accuracy;       2. Procedures for correcting errors. 2. **Scope**    1. This procedure includes in its scope all data which we process either in hardcopy or digital copy this includes special categories of data.    2. This policy applies to all staff, including temporary staff and contractors, and volunteers who process personal data. 3. **Data accuracy procedures**    1. In line with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 Barnardo’s will “maintain securely an accurate and complete record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided”.    2. Barnardo’s staff and volunteers will ensure accuracy in the data in both hardcopy and digital records by making sure all data has the following characteristics:       1. Authentic – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed;       2. Reliable – i.e. the data is complete, accurate, has been created within 5 working days, 24 hours in respect of safeguarding, of the activity it records, and the data has been provided by individuals with direct knowledge of the event it records;       3. Integrity – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified;       4. Useable – i.e. the data can be located when it is required for use and its context is clear.    3. The principal purpose of service user records is to record and communicate information about the individual and their care, to plan and review the intervention and to measure impact. The principal purpose of staff records is to record employment details for payroll and business planning purposes and to support and develop staff.   To fulfil these purposes:   * + 1. Standardised structures and layouts are used for the contents of records; see Children’s Services and Business Lines Recording policy, when recording using Barnardo’s recording systems Eclipse or Content Server SUR. Services that record on 3rd party systems are required to adhere to the requirements of those organisations, which are compliant with requirements of GDPR.     2. Documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order;     3. A plan is produced and regularly reviewed and shared with everyone involved;     4. Staff and volunteers who process personal data are inducted on the creation and use of records (see Service Recording Policy, Practice Guidance for use Of Content Server SUR and Eclipse and Charms).     5. Have implemented a procedure that enables service users and staff to have easy access to their records where appropriate. This is outlined in the Privacy Notices, Your Data, Your Rights Leaflet, Data protection and Recording Policies.   3.4 All staff who record information - whether hardcopy or electronic - have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access to.   1. **Procedures for the correction of errors**    1. In-line with GDPR, individuals have the right to have access to their personal data. They have the right to the rectification of said records in the instance that their records are inaccurate or incomplete. Factual data will be updated, the recording of contacts, meetings etc. will not be amended but any disagreement about the content will be noted on the record.    2. Where at all possible, in the instance that we have appropriately shared that individual’s records with any third-party, we will inform this third-party of the rectification if appropriate.    3. In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.    4. To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.    5. In the instance where the rectification request is refused**,** the reason will be explained in full and in writing within one month of the original request having been received.    6. A record of all rectification requests and outcomes will be recorded on the data subject’s record.    7. All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO;    8. All staff will be informed of this procedure in the Recording policy (not sure about staff records).    9. All service users, or their legal representative, will be informed of this procedure, as well as their other rights as regards their personal data, in the Privacy Notices and Your Data, Your Rights Leaflet.    10. In order to process requests for rectification of data , the subject will be asked to provide identifying documents so that we can authenticate that it is appropriate for their data to be amended. 2. **Responsibilities**    1. The Assistant Director Data Protection and Data Governance has overall responsibility for policies and procedures being reviewed annually.    2. The Service Manager has responsibility for staff training in data quality and for monitoring data quality throughout the service. They also are responsible for responding to rectification requests and recording the outcome of any request.    3. The Service Manager is responsible for the quality of records and making sure that staff understand their commitments in ensuring data quality.    4. Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice to the Service Manager.    5. Staff members are aware that data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action. | |
| 1. **Risk Assessment** | |
| The Policy Owner, with assistance from relevant individuals, will undertake a detailed risk assessment of risks facing Barnardo’s which impact on recording at least every 2 years, using this to inform required changes to this Policy, any associated processes and procedures or training/awareness messages as required. | |
| 1. **Compliance and Oversight** | |
| It is the responsibility of **Directors** and **Heads of Departments** to ensure that the recording of service user, carer and supported lodgings provider recording is undertaken in line with this policy. As part of their quality assurance role ADCSs or equivalent will assure themselves that the recording provided is of sufficient quality. | |
| 1. **Document History** | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Version** | **Date** | **Author** | **Status** | **Approval (by / when)** | **Comments** | | 1 | 7/10/19 | Pat Greene | Draft | For approval by CSMT on 22/10/19 | Approved by CSMT 2019 | | 2 | 11/11/19 | Pat Greene | Approved | CSMT on 22/10/19 | Replaces previous recording policy. | | 3 | 11/10/20 | Pat Greene | Reviewed | NA | No amendments made. | | 4 | 11/5/21 | Kate Goodwin | Reviewed | NA | Broken links refreshed  References to archived leaflets removed | | |

**Appendix 1**

**THE RECORDING OF SERVICE USER/CARER/SUPPORTED LODGINGS PERSONAL DATA**

**Please note this table addresses the recording of data on Barnardo’s systems, where commissioner’s or partner’s systems are used the appropriate policies, procedures and protocols must be followed.**

| **Type of Data** | **Where this should be stored** | **Legal Basis for Processing** | **Retention Period** | **Responsibility for Management and Deletion of Data** | **Any other requirements** |
| --- | --- | --- | --- | --- | --- |
| 1.**Referral** prior to assessment or offer of service | The referrals area in Eclipse or Charms,  Referral cabinet in Content Server SUR. | Public task  Legitimate Interest  Consent obtained by referrer. | 1 year from receipt, unless there is a contractual requirement to retain for longer.  All data must be deleted from Content Server prior to closure of service/cessation of contract. | CSM responsible for sending lists of data to Digital for deletion or deleting data from content server when retention date is reached, responding to SARs or information sharing requests in relation to data. | Referring agency must have informed data subject that their data has been shared with Barnardo’s or subject given Privacy Notice and Your Data, Your Rights form if referral is direct to service. |
| 2**. Referral** once service delivery begins or initial assessment undertaken. | Case file opened in Eclipse, Content Server SUR or Charms. | Public task  Legitimate Interest | Retention period as specified in Retention Grid and identified in the Service Recording Protocol. | CSM responsible for sending lists of data to Digital for deletion or deleting data from content server when retention date is reached, responding to SARs or information sharing requests in relation to data, while service is open. Once service closes responsibility lies with locality ADCS or making Connections. | Data subject /s to be given Privacy Notice and Service Information Form when service delivery begins or initial assessment undertaken. |
| 3. **Direct casework** with service user or direct work with parent carer on service users behalf where there is data to be recorded about the service user. | **Case file** opened in Eclipse, Content Server SUR or Charms in respect of service user.  **Case file** opened in respect of parent/carer if there is personal data to be recorded about them.  **Case file** opened in Eclipse in respect of family members. | Public task  Legitimate Interest | Retention period as specified in Retention Grid and identified in the Service Recording Protocol. | CSM responsible for sending lists of data to Digital for deletion or deleting data from content server when retention date is reached, responding to SARs or information sharing requests in relation to data, while service is open.  Once service closes responsibility lies with ADCS or Making Connections. | Data subject /s to be given Privacy Notice and Service Information Form when service delivery begins, unless this has already been provided.  Each data subject must have an individual case file with core data form. |
| 4. **Open Group work recording when the members of a group do not have an individual case file.** This will include copies of attendance lists, group members, and information about group work activities. | **Group file** to be opened SUR Confidential folder in Content server.  If **Safeguarding** concerns identified about any member of the group an individual case file SUR or Eclipse must be opened. | Public task  Legitimate Interest | **6 years from last recording** | CSM responsible for sending lists of data to Digital for deletion or deleting data from content when retention date is reached, responding to SARs or information sharing requests in relation to data.  Once service closes responsibility lies with locality ADCS. | This will replace the recording of this information in the group work cabinets in content server SUR. |
| 5. **Closed Group work**- when group members do have individual case files. | Individual case files opened in SUR or Eclipse | Public task  Legitimate Interest | Retention period as specified in Retention Grid and identified in the Service Recording Protocol | CSM responsible for sending lists of data to Digital for deletion or deleting data from content server when retention date is reached, responding to SARs or information sharing requests in relation to data, while service is open. | SUR Data copied across to individual case file when subject attends group.  Eclipse process to be identified. |
| 6. **Foster carers/adopters** | Individual **casefile** in Charms. | Public Interest  Legitimate Interest | **Statutory Retention Period** | **To be identified** |  |
| 7. **Adoption support** | Individual **case file** in Charms. | Public Interest | **Statutory Retention Period** | **To be identified** |  |
| 8. **Supported Lodgings Providers** | Individual **casefiles** to be opened for each provider in SUR or Eclipse. | Public Interest  Legitimate Interest | **75th birthday** | CSM responsible for sending lists of data to Digital for deletion when retention date is reached, responding to SARs or information sharing requests in relation to data, while service is open. |  |
| 9. **Involvement in care planning/risk management planning with no direct contact with service use** | **Case file** to be opened SUR Confidential folder in Content server. | Public interest as delivered through Government contract | **19th Birthday** | CSM responsible for deletion of data when retention date is reached, responding to SARs or information sharing requests in relation to data, while service is open. Once service closes responsibility lies with locality ADSCS. | Barnardo’s privacy notice/Your Data, Your Rights provided by LA worker on Barnardo’s  behalf |
| 10. Records of **advice provided to professional** used to provide anonymised data to commissioner or link to previous advice provided. | Minimum amount of personal data held on data base in SUR Confidential folder in Content server | Public interest as required to deliver a contract | **12 months** after providing advice or **12 months** after reporting. Retention date to be included in name of file or folder. | CSM responsible for deleting when retention date is reached or service is closed. | LA privacy notices to include data sharing with other agencies. |
| 11. **Personal data which is a duplicate of data held on service user record.** This will include personal data that has been collated in order to report to commissioners or to manage the service delivery | The data may be held on a spreadsheet or in other formats, but it must also be held on the service user record in core data or in contacts or in a report. Must be saved **in SUR Confidential folder in Content server** | Public task  Legitimate Interest | The data must be deleted when it is no longer needed, e.g. when the data has been reported on or at the end of the contract or if the service closes. Retention date to be included in name of file or folder. | CSM responsible for deleting when retention date is reached or service is closed. |  |
| **12. Personal data which needs to be retained for a short period only.** This includes personal data that is not recorded on other systems but only needs to be retained for a short period, i.e. up to two years or the lifetime of the contract, and does not meet the criteria for opening an individual or group file. This could include pre-referral forms, complaints about the service that are not covered by the Complaints Policy or subject access requests when there is no record on which to record the request. | The data may be held on a spreadsheet or in other formats, but it must also be held on the service user record in core data or in contacts or in a report. Must be saved to SUR **Confidential folder in Content server.** | Public task  Legitimate Interest | There must be a retention date identified and the data must be deleted when that date is reached. Retention date to be included in name of file or folder. | CSM responsible for deleting when retention date is reached or service is closed. |  |
| **13. Personal data held by regional or national or business line offices.** This will include records of complaints, subject access or information sharing requests or safeguarding issues where the data subject does not have a record in an active file room. This will replace the proposed file room for R/N/BL offices. The data must have a retention date and must be deleted when that date is reached. | Must be saved to SUR **Confidential folder in Content server.** | Public task if related to delivery of contract  Legitimate Interest for other data | There must be a retention date identified in the name of the document. The data must be retained for as long as it is required. This would normally be 12 months from last recording unless it involved safeguarding where we are not involved in a plan or complaints when it would be 6 years unless there is a reason to retain longer identified by the manager. | Director responsible for identifying someone to ensure data is deleted once retention date is reached and check if there is a SAR or information sharing request. |  |