

Meadows School

London Road, Southborough, TN4 0RJ

enquiries@meadowsschool.org.uk

Service Recording Protocol

Table of Contents	
Monitoring & Review	Page 1
Data Protection Impact Assessments and Information Sharing Agreements	Page 2
Location of Personal Data Recorded by the Service	Pages 3,4,5&6
Referrals/Requests for Service	Page 6
Core Data/Local Data Form	Page 7
Assessment, Planning, Review	Page 8
Recording Templates or Service Specific Guidance	Page 8
Outcomes	Page 8
File Sign Off and Sampling	Page 9
Case Closure/Retention Periods	Page 9
Recording of Group Work	Page 9
Photography, Audio and Video Recording including CCTV	Pages, 10, 11,12&13
Obtaining Parental Agreement to Provide a Service	Page 13
Data Protection & Security	Pages 14,15&16
Appendix A – Service Data Flow	Page 17

Name of Commissioner/s	Who is the Data Controller
Various Local Authorities – each service user has a separate contract	Meadows School – Barnardo’s

Monitoring and Review

This addendum is monitored annually by the school’s Data Manager to ensure compliance with both Barnardo’s policy and the DfE guidance.

It should be read in conjunction with Barnardo’s Data Protection Policy (updated every 3 years)

<p>Has a Data Protection Impact Assessment/s been completed in respect of all of the recording undertaken by the service? This is an assessment of the systems and processes used to process data to ensure that they are GDPR compliant.</p>	<p>Does the Children's Services Standard DPIA for Recording on Barnardo's systems apply to all of the personal data processed by the service?</p>	No
	<p>Has the service data flow in relation to this been completed?</p>	Yes – Appendix A
	<p>Does the Children's Services Standard DPIA for Recording on Commissioner's systems apply to any of the personal data processed by the service?</p>	No
	<p>Has the service data flow in relation to this been completed?</p> <p>If Yes has a copy of the commissioners DPIA or evidence of due diligence checks been obtained?</p>	N/A
	<p>Is there a DPIA for any personal data processed by the service that is not covered by the Children's Services Standard DPIAs?</p> <p>If Yes list the names of DPIAs completed and location if not on One Trust.</p>	<p>Yes</p> <ul style="list-style-type: none"> • Arbor DPIA Meadows School Sharepoint (365) DPIA
<p>Are there Information Sharing Agreements in place in relation to some or all of the information sharing undertaken by the service? If Yes, please list the agreements stating who they are between and which data they relate to.</p>		<p>Yes – an Information Sharing Agreement with each Local Authority that we work with and the DfE</p>
<p>Is the service required to be compliant with the NHS Data Protection & Security Toolkit?</p>		No

Location of Personal Data Recorded by the Service

Arbor

Arbor is the school's Management Information System, this is where all core data about service users is stored. All statutory documents should be stored here. CPOMs is linked to Arbor for up-to-date core information. We use Arbor to track academic progress and write academic reports. This is where the daily register is taken which is a legal requirement for the school and where the DfE census is taken from 3 times a year - it is linked to the DfE portal for this (Collect). All child-facing staff and admin have access to Arbor.

Young Person's information

Each young person has their own record which has the following information:

- Personal – All contact details for the young person are stored here (family SEN, Social Care, emergency contacts etc) home address, phone number, email address.
- Names – Legal name and any other known names
- Entitlement – Free School Meal Eligibility, Pupil Premium status and other relevant entitlements
- Enrolment – date of admission, whether enrolled in any other provisions simultaneously, whether day or resident pupil
- Attendance – overview of attendance at school and at previous schools
- Additional – data on ethnicity, language spoken, what educational funding they are entitled to, Care Orders, Child Protection register, whether they are a service child, traveller, whether they are out of Authority.
- Medical – GP surgery, any medical conditions that require support.
- Groups – used for reporting purposes to select specific types of Young Person.
- Docs & Comms – all statutory documents that must be retained by the school, initial referral papers, Annual Review reports, Behaviour Support Plan and Individual Risk Assessment, Consent forms, EHCP, Therapy reports/assessments, School reports, Reports from external professionals (I.e. Educational Psychologist reports), Offer letter.
- Movements – which schools the young person has moved from and to
- SEN – specified SEN needs
- Parental Consent – overview of what consents are in place and when received.
- Assessments – for teaching assessments, not currently used.
- Exams – candidate number and ID

Arbor is a management information system that shares data with other systems (CPOMS and DfE) and also what the school uses to complete the statutory Census for the DfE each year.

Location of Personal Data Recorded by the Service - Continued

CPOMS

CPOMS is used for our Child Protection records. It works as a data base as well and is linked to Arbor for up-to-date staff and students. It is a chronological data base that can also sort and analyse to ensure that no element of safeguarding is missed.

- Overview – contains data drawn from Arbor I.e. class, unit, legal status etc
- Incidents – chronological record of all safeguarding incidents recorded for the young person.
- Contact details – relevant contacts drawn from Arbor
- Document Vault – all scanned documents that have been uploaded for the young person
- Library – Record of confidential safeguarding meetings
- Attendance – attendance data drawn from Arbor.
- Student Report – this provides a reporting function where users can filter incidents with various parameters such as category, date, external professionals involved.
- Audit report – full audit of who has accessed the young person's file, when and what they have accessed.
- Monitoring history – overview of reports and what categories they come under

The system provides a facility for Child Protection records to be transferred from previous school and for Meadows to transfer our Child Protection records to the next provision the young person attends (in line with statutory duty under Keeping Children Safe in Education).

CPOMS also has a reporting function where reports on records can be run based on various different parameters.

Planner – staff can set reminders and events pertinent to Child Protection records I.e., a reminder to follow up an event.

Library – this is used to store records of confidential safeguarding meetings

Dashboard – each member of staff has an individual dashboard, staff are alerted to appropriate reports and actions that are required of them, this appears on the dashboard and is removed when completed (marked as read)

Access to records on CPOMS is controlled, only staff who have permission can access records. Any access to any record is timestamped and can be audited. Ability to edit records is restricted to certain staff and all edits are auditable with original versions kept on the system.

Location of Personal Data Recorded by the Service - Continued

Microsoft 365

The school have several groups for different areas of the school and access is granted accordingly. All staff and governors have access to relevant areas of SharePoint with access approved by SLT. Staff are also given access to apps relevant to their role. All staff have access to Outlook and their personal OneDrive.

- **WholeSchool Group** - All staff and governors have access to read items in group but only a selection of staff can edit the group site or documents on it. Some areas of the group are editable for everyone and this is completely controllable down to the individual file.
Contains:
 - Student file room
 - Annual review Information
 - BSP
 - IHP
 - Teaching and Learning resources
 - Induction Information and Staff Handbooks
 - General Information for all staff
 - Policies & Procedures
 - Staff group working areas

- **FileRoom Group** – All child-facing staff and admin have access. This is a storage area for documents on individual students (similar to content server fileroom). The FileRoom is being phased out as we utilise Arbor functions more. FileRoom is built inline with Barnardo's retention policy and staff cannot delete documents once saved.

- **Confidential to SLT** - Only SLT have full access, some admin staff have been given individual access to areas that they support.
Contains:
 - Single Central Record
 - SEF and SDP
 - Staff issues
 - HR & Recruitment
 - Finance

Paper Based Records

Main Office

Contains:

- Exam papers – locked in safe upon arrival and when ready to be collected.
- On occasion safeguarding files are posted to the school, these are scanned and added into CPoMs immediately, the originals are shredded. Relevant staff are then informed that an electronic copy is available.

Location of Personal Data Recorded by the Service - Continued

Data recorded using Barnardo's systems

Young people who started at the school before September 2021 will have information recorded in the Content Server file room. A note has been added to each child's Arbor file to indicate records are also stored on content server. A note has been added to each child's Content Server file to indicate records are also stored in Meadows Systems.

Data recorded using commissioner's or partner's systems

Young people who are Children in Care have Personal Education Plans, local authorities ask for these to be recorded on their central portal called an EPEP system. A copy is kept in Arbor.

Data recorded in SUR confidential folders in Content server

Young people who started at the school before September 2021 will have information recorded in the Content Server file room. A note has been added to each child's Arbor file to indicate records are also stored on content server. A note has been added to each child's Content Server file to indicate records are also stored in Meadows Systems.

Referrals/Requests for Service

On receipt of a referral by post or email, details are logged on the school's Referral Spreadsheet. The file is stored in a secure digital location (FileRoom –M365) for review by the Referrals Panel (or other appropriately delegated member of staff) in terms of the young person's profile, placement suitability and availability. Where necessary, a follow up telephone call to the placing authority may be required to obtain further information.

Referral discussion outcomes are agreed formally, regularly by the Principal.

Visits by representatives from the placing authorities, parents/carers, young person and any other relevant involved professionals are organised. Taster days for some potential students will be arranged.

When these visits have taken place and it has been agreed that the placement would be appropriate, an Offer Letter is sent to the Local Authority outlining fee structures and type of provision. On agreement by the Local Authority, a start date is agreed with the parent/carer, copying in the Local Authority and any other relevant involved professionals.

On the young person's start date, an Admissions Meeting is convened where information is shared, consents completed, and initial targets set. On the day of admission, core information is entered onto Arbor by the school office and a folder is created in M365 Student File Room. The core data is automatically linked to CPOMS. A student log in is created for the young person by the IT Team.

It is a Department for Education requirement that information equivalent to core data is maintained on a Management Information System used for the school census (currently Arbor).

Hard copies of referral papers are scanned and stored in the FileRoom (M365) and recorded on a spreadsheet. Referrals who don't become placements are deleted from the FileRoom automatically (PowerAutomate) after 3 months. Referrals that become placements are moved to the FileRoom group where an individual file is created.

Core Data/Local Data Form

Arbor

Arbor is the school's Management Information System, this is where all core data about service users is stored. All statutory documents should be stored here. CPOMs is linked to Arbor for up-to-date core information. We use Arbor to track academic progress and write academic reports. This is where the daily register is taken which is a legal requirement for the school and where the DfE census is taken from 3 times a year - it is linked to the DfE portal for this (Collect).

Young Person's information

Each young person has their own record which has the following information:

- Personal – All contact details for the young person are stored here (family SEN, Social Care, emergency contacts etc) home address, phone number, email address.
- Names – Legal name and any other known names
- Entitlement – Free School Meal Eligibility, Pupil Premium status and other relevant entitlements
- Enrolment – date of admission, whether enrolled in any other provisions simultaneously, whether day or resident pupil
- Attendance – overview of attendance at school and at previous schools
- Additional – data on ethnicity, language spoken, what educational funding they are entitled to, Care Orders, Child Protection register, whether they are a service child, traveller, whether they are out of Authority.
- Medical – GP surgery, any medical conditions that require support.
- Groups – used for reporting purposes to select specific types of Young Person.
- Docs & Comms – all statutory documents that must be retained by the school, initial referral papers, Annual Review reports, Behaviour Support Plan and Individual Risk Assessment, Consent forms, EHCP, Therapy reports/assessments, School reports, Reports from external professionals (I.e. Educational Psychologist reports), Offer letter.
- Movements – which schools the young person has moved from and to
- SEN – specified SEN needs
- Parental Consent – overview of what consents are in place and when received.
- Assessments – for teaching assessments, not currently used.
- Exams – candidate number and ID

Assessment, Planning, Review

When a review or significant meeting is held the information is uploaded to Arbor, or CPOMS if relating to a safeguarding or child protection issue. Any reports must be recorded on the forms found in 'Templates' in WholeSchool Group.

Therapeutic and Cognitive Assessments

These are standardised tests used to give baseline, and mark progress in a range of SEMH and cognitive fields. The results are recorded on a template and results used to inform practice. This could be a regular assessment or part of an adhoc requirement, including being commissioned as part of the Annual review of EHCP.

Academic Assessment

Assessment mark books are created in Arbor to track academic progress through the curriculum.

A short report is produced for parents/carers (and/or local authority) at the end of Terms 2 & 4 – saved in Arbor. A full academic report is produced for parents/carers (and/or local authority) at the end of Term 6 – saved in Arbor. Mark books are assigned to the relevant teachers in that particular year group.

Academic reports to parents, along side parents evenings, are part of a legal duty to report progress.

Annual Review of EHCP

This is a legal requirement to review the Education, Health and Care Plan, often in a multi-agency meeting. The reports compiled before the meeting and the headteachers report post meeting are on a specific template.

Recording Templates or Service Specific Guidance

The school has obligations to meet requirements from several different agencies when recording information. The school has a duty to create, use and amend templates that meet these requirements:

- Mandatory Policies for Schools
- Department of Education Guidance
- Keeping Children Safe in Education

Outcomes

Individual outcomes are recorded in Arbor and are monitored both individually and in relevant groups from there.

Education outcomes are reviewed termly (6 times per year)

EHCP outcomes are measure 3 times per year (at the end of Terms 2,4&6)

All child-facing staff are aware of each student's targets and senior leaders work with the relevant teams to ensure progress is being made.

File Sign Off and Sampling

File Sign Off involves the reading of the case records by the immediate Tutor and Linkworker to understand the work that is being undertaken with a service user, as well as ensuring that the records meet the requirements of the Recording Policy and that the content of the record is of the standard required. Files are checked twice a year – at the end of Terms 3 and 6.

File Sampling is a quality assurance process undertaken by the **Principal** if they are not the immediate line manager. Ten percent of the case files are sampled to ensure that they meet the Recording Policy and are of the required standard. File sampling is recorded in the Confidential to SLT File (M365)

Case Closure/Retention Periods

All information stored on students is kept in line with Barnardo's current retention policies.

FileRoom (M365) has an automated system to remind admin staff if a file is nearing deletion – Retention dates are set automatically upon key words being used (Safeguarding/BIRF etc) and the DSL is alerted should a retention date change.

Arbor has an automated system to remind admin staff if a file is nearing deletion – Education records are kept for 6 years after a student has left. Should any information need to be kept longer (due to Barnardo's policy) a copy of the Arbor file is downloaded and kept in Fileroom.

CPOMs – safeguarding files are kept for 75 years from Date of Birth (in line with Barnardo's policy).

Closure summaries are kept in Arbor – schools are required to report on leavers for up to 6 years after they leave.

Recording of Group Work

Group work is delivered in the school (both lessons and therapies) but observations, notes and outcomes are recorded individually.

Photography, Audio and Video Recording including CCTV

Photography and Sharing Images Guidance

It's important that children and young people feel happy with their achievements and have photographs and films of their special moments.

We recognise that:

- Sharing photographs and films of our activities can help us celebrate the successes and achievements of our children and young people, provide a record of our activities and raise awareness of our organisation.
- The welfare of the children and young people taking part in our activities is paramount.
- Children, their parents and carers have a right to decide whether their images are taken and how these may be used.
- consent to take images of children is only meaningful when children, their parents and carers understand how the images will be used and stored and are fully aware of the potential risks associated with the use and distribution of these images.
- there are potential risks associated with sharing images of children online.

We will seek to keep children and young people safe by:

- Only using school owned equipment to take the photos and all cameras and memory cards kept securely until downloaded and wiped clean
- If professional services used to take photos or videos, agreement is made before hand about who owns the image and where they will be process and stored.
- Asking for permission and getting written consent from the school before taking, using and storing photographs that include images of children.
- Always explaining what images will be used for, how they will be stored and what potential risks are associated with sharing images of children.
- Making it clear that if consent is withdrawn for an image to be used or shared after it has been published, it may not be possible to delete images that have already been shared or published.
- Never publishing personal information about individual children.
- Using images that positively reflect young people's involvement in the activity.

Photography and/or filming for personal use

When children themselves, parents, carers or spectators are taking photographs or filming at our events and the images are for personal use, we publish guidance about image sharing in the event programmes and/or announce details of this guidance before the start of the event. This includes:

- Asking for photos taken during the event not to be shared on social media
- Recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share
- Reminding children, parents and carers who they can talk to if they have any concerns about images being shared.

Photography, Audio and Video Recording including CCTV - Continued

Storing images

We will store photographs and videos of children securely, in accordance with our and data protection policy.

- Hard copies of images are only used inside secured notice boards around the school
- electronic images are stored in an image library with restricted direct access.
- We will never store images of children on unencrypted portable equipment, such as laptops, memory sticks and mobile phones. Ideally cameras or devices belonging to the school should be used.

Meadows School Use of CCTV

Statement of Intent

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with all data protection legislation, including the Data Protection Act 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

The school has a surveillance system for the purpose of:

- Supporting safeguarding and child protection
- Prevention and detection of crime
- Promotion of health, safety and welfare of staff, pupils and visitors

This includes utilising the system as an objective reference when reviewing footage for the purpose of investigation e.g. allegations, injuries, misconduct, negligence.

It will not be used to monitor the day-to-day performance of staff but it would be used to review staff actions under any of the above circumstances. It will not be used to supervise young people.

Photography, Audio and Video Recording including CCTV - Continued

Using the Cameras and Monitoring of Data

The school has extensive Closed Circuit Television (CCTV) which operates 24 hours a day within school buildings and around the school campus. Most internal cameras have audio capability. This is turned on if deemed necessary in the review of an incident as most antecedents to an event are verbal (auditory) rather than physical (visual).

Visual display monitors for external cameras are located in the main office.

Full access to the surveillance system, software and data will be strictly limited to authorised operators who have individual, password protected, and only accessible through individual logins. Although the system uses the network infrastructure to carry data, the system is stand alone and is not part of the school networked systems.

The school's authorised CCTV system operators are:

- SLT
- IT Team – for support purposes only
- Premises supervisor – for support purposes only
- Head of Key Stage 2 – provision offsite to main school

The footage is used to review incidents (Safeguarding, Behaviour, Health and Safety) when necessary, to ascertain what happened, to clarify events, review to prevent a re-occurrence and therefore ensure all persons are kept safe. The review also enables a unique experience as a learning and development tool for all staff.

The CCTV form is completed by a system operator each time CCTV footage is viewed. An audit of the CCTV access will be carried out by the DSL and Principal on a half termly basis.

Privacy by Design

- Effective Signage will be in place at the entrance to the site and in Key locations around the site making all pupils, staff and visitors aware of the use of CCTV.
- All young people, parents/carers and placing authorities/professionals will be made aware of the CCTV policy in their admissions meeting at the school and will be asked for their consent prior to beginning their placement at the school.
- All visitors to the school are made aware that the school use CCTV and an explanation of why and how this footage is used will be displayed on arrival when they sign in.
- CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose
- The school will make every effort to position cameras so that their coverage is restricted to the school premises, both indoor and outdoor areas.
- The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.
- Footage is held for 31 days before being automatically deleted. Sections can be saved for longer if needed for evidence in an investigation. Any saved footage will be deleted once it is no longer needed.

Photography, Audio and Video Recording including CCTV - Continued

Access to and Disclosure of Images to Third Parties

- There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators)
- Requests should be made in writing to the Principal.
- The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

Obtaining Parental Agreement to Provide a Service

The person with Parental Responsibility (PR) should attend the Admissions Meeting. If the child is subject to a full care order and the local authority has PR, a person with delegated authority to sign consent on behalf of the local authority can do so (this would usually be the child's allocated social worker). If in any doubt about who/how to get consent this will be discussed with a member of the Senior Leadership Team.

Care is taken to only store relevant information that helps with the care of the child and the running of the school. Duplication of data is reduced by using digital systems that everybody can access. Data is destroyed when no longer necessary in line with Barnardo's and Meadows protocols as set out in our privacy notices in relation to GDPR.

Signed consent forms are scanned and saved in FileRoom. Parental Consent tab is updated on Arbor.

Data Protection and Data Security

Informing the Subject that a Record of their Personal Data is Being Kept

On admission, the person with parental responsibility is informed that records will be maintained on their child and their consent is obtained. They are provided with 'Your data, your rights' information leaflet.

Obtaining Consent if this is Required

Parent/Carer consent is obtained at the admissions meeting at the start of the placement. There is consent for the child to access the service plus additional consent for specific elements including:

- Therapies Informed Consent
- CCTV Consent
- IT Acceptable Use Agreement
- Trips and Activities Consent
- Photography and Sharing of Images – Unless for use around the school this is sought for each individual image when used
- Working with parents/carers – Home /School agreement
- First Aid Consent including homely remedies

Contacting Service users to Provide Information About Services or Seek Feedback

We collect feedback from service users over time including surveys and during conversations. We do not contact service users after they have left for feedback. Large scale school surveys do not gather identifiable personal data and do not need to be stored with individual files.

Data Protection and Data Security - Continued

Subject Access and Information Sharing requests

Service users, parents and carers have the right to request copies of their data and this must be provided to them within a month of receipt of the request or 15 school days. The request must be in writing. Information sharing requests may be received from third parties, such as the police. These must be reported to the Principal/Data Manager as soon as they are received.

When a Subject Access Request is made the Data Manager will be designated as responsible for gathering the data from different systems.

CPOMS – a report will be created from the young person’s records. All other names will be redacted and the DSL’s will check whether there is any sensitive information that should not be disclosed due to concerns about the impact on the young person. If there are concerns about disclosing information the school will seek legal advice from Barnardo’s legal team about what to disclose.

Arbor – a report will be created by the schools Data manager, this is checked and redacted if needed

Microsoft 365 – a member of staff will be nominated to ensure all data from Young Person’s fileroom and Young person’s folder in the unit SharePoint is downloaded and saved in a report. This information is checked by the Data Manager and redacted if necessary

If a child has records on content server (if they were a pupil at the school before September 2021) a member of staff will be nominated to ensure all data from the young persons content server file room is downloaded and saved in a report (information will be checked to ensure it is not a duplicate from other systems). If necessary, the report will be redacted to protect the personal information of other service users.

Paperbased records – the Data Manager will contact the Making Connections Team so that they can check for a paper archive and prepare for reporting. This information is checked and redacted if necessary

A record of what has been shared for each Subject Access Request will be kept by the school, monitored by the Principal and reported to Barnardo’s through OneTrust.

Data Breach Reporting

All data breaches must be reported immediately when they are discovered by completing the Form in OneTrust. A record of the breach and any correspondence will also be kept in the Confidential to SLT Group (M365). Obtaining additional information must not delay the reporting of the breach, additional information may be added later.

The Data Manager should be informed immediately but this must not significantly delay the reporting of the breach if they are not available in the event of a data breach or suspected breach. The school will notify the relevant Local Authority if there is a breach of security relating to personal data.

Data Protection and Data Security - Continued

Security of Personal Data

Only electronic copies of files may leave the site. No hard copies of information are removed.

Staff must only access these files on a device provided for them by the school and the following additional security applies:

Arbor – Only accessible by child-facing staff with permissions applied to access information against their job role

M365 -Sign in requiring a 15 character password to sign in – staff who have access to the background of the system require MfA through Microsoft Authenticator.

CPOMs – Secure Sign in with two factor authentication – only designated staff can access

All sign ins are audited on the individual system and audited for unusual access

Email and Letters

Emails are an integral part of M365 which by its nature reduce the need for attachments or personal information to be in the body of the email. Emails sent within the Meadows domain are already protected and do not need to be encrypted. Meadows have forced TLS encryption to the Barnardo's email domain. This means all email will be transported through an encrypted channel between the 2 domains. Emails sent to other external domains containing personal data are manually encrypted using M365.

If personal data is sent out by mail, return contact details are added to the envelope and, where appropriate, recorded delivery must be used.



Meadows School

Data Flow Diagram

