Walsall Council

Walsall Children's Services
Better Together for Children

Data Protection and Records Management

Contents

1. Introduction
2. Case Recording
3. Confidentiality
4. Access to Records
5. Complaints / Appeals
6. Documents to be Routinely Sent to Service Users
7. Public Information on Policy and Practice
8. Management of the Policy

Appendix 1: Eight Principles of the Data Protection Act 1998

1. Introduction

This policy reflects the requirements of the following legislation:

- Data Protection Act 1998;
- Human Right Act 1998;
- Freedom of Information Act 2000.

It is also consistent with the common law duty of confidentiality and the **Caldicott Principles**. The policy is in line with Walsall's Information Governance Policy Framework which is intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Council and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery to customers (see Information Governance Policy Framework on the Walsall Council website).

This document applies to both paper and electronic records.

All case recording should promote the key principles of partnership, openness and accuracy, and should be seen as part of the overall service to the child and his/her family, and to approved carers (see **Appendix 1 - Eight Principles of the Data Protection Act 1998**).

Records of assessments will be routinely given to children and their parents, and to applicants for approval as foster carers or prospective adopters

2. Case Recording

2.1 Definition of a Case Record

A case record is the account of work undertaken with an individual child, his/her family or with an adult, for example a foster carer or prospective adopter, by Children's Social Care, and includes:

- Paper files;
- Electronic records (Mosaic);
- Video recordings;
- Audio recordings.

The Fostering Service and Adoption Service will keep paper in relation to carers. However, when a worker from the Fostering or Adoption Service has seen a child in placement they will add a case note on the child's record which relates to the child in placement. This **must not** be an adult/carer focused case note.

All case records are the property of Walsall Council.

The case record will include copies of all information given to the individual.

2.2 Purpose of Recording

Record keeping is an important and fundament part of our business for the following reasons:

- It supports effective partnerships with children, their families and approved carers;
- It ensures an accurate, documented account of the involvement of staff working in Children's Social Care with individual children, their families and approved carers;
- It provides the child's story and incorporates the wishes and feelings of the child during involvement of Children's Social Care;
- It provides a basis for assessments and decision making;
- It assists continuity when workers are unavailable or change;
- It provides an essential tool to enable work to be monitored and audited.

2.3 Legitimate Basis for Obtaining and Using Information

Children and their families have a right under the Data Protection Act 1998 to be informed about the case records kept about them, the reasons why, and their rights to confidentiality and of access to their records.

Any person from whom personal information is collected will be advised, therefore, of the following at the time the information is obtained:

- The identity of the person or organisation to whom they are giving information;
- How their information will be used;
- The identify of any person or organisation with whom the information may be shared.

2.4 File Structure and Maintenance

Each child will have one case record, which may contain a number of modules. The exception will be where the child has an adoption plan, in which case an **Adoption Case Record** will be opened and kept separately.

Paper files will be destroyed and electronic records deleted in line with Children's Social Care's agreed retention schedule

2.5 Content of Case Records

The content of all records should reflect the principles of good recording practice and should demonstrate the basis of the professional decision making process.

Those completing electronic records **must** input their name and date stamp when the recording was completed. Where paper records are kept, they should be typed and all records must be signed and dated with the name and role of the author clearly legible (with author's name printed under their signature).

Only information that is necessary and relevant will be recorded.

All steps will be taken to ensure that any personal information is recorded accurately and kept up to date on Mosaic and in any paper files. There must be a clear distinction between facts, analysis and professional opinion as a worker. This must be clearly recorded and distinguished with appropriate sub-headings.

Any information recorded needs to be clear in order that others can understand, make decisions and act on it.

All records should include a statement regarding the purpose of Children's Social Care involvement with the individual.

Decisions made in supervision are a significant part of the case record and they should be clearly recorded on a Management Decision Record (MDR) and held on the main file as an integral part of the record. If the supervision record is on a paper file, it must comply with the guidance above.

All other Managers' decisions that relate to a child or the applicant for fostering/adoption must be recorded on an MDR on the case record.

Case records should be summarised in a **Chronology** of significant events, in accordance with the Guidance Notes for Compiling Chronologies.

The views, wishes and feelings and aspirations of children, their carers and **Advocates** should be recorded, particularly in all **Assessments**, child permanency reports, and court reports but also in general case recording of visits to children.

Records should demonstrate that the needs of children, their families and carers have been assessed with account taken of race, culture, religion, disability, gender, sexuality and age and any other factors that impact on them.

Recording must evidence an analysis of the risks to the child and options for reducing them.

Review reports will evidence the involvement of the child and parents, carers, statutory agencies and service provided (public and independent) at all relevant stages.

Professional disagreements, when they occur, must also be recorded appropriately using provided guidance and must not be entered on to the child's file as this is inappropriate.

It is important that referrers are informed of the outcome of their referral, and the fact that this notification has taken place should be recorded on Mosaic.

3. Confidentiality

3.1 Maintaining Confidentiality

All information regarding children and their families will be treated as confidential and only be available on a "need to know" basis, which means that:

- Staff will only access information that is essential in order for them to undertake work with or on behalf of a particular child;
- Any member of staff accessing records containing personal information about the subject without a justifiable reason may be subject to disciplinary action;
- Paper records must be kept in a secure filing system to control access;
- Personal information about children and families will be only be shared with a third party with the person's informed consent, unless there is a legal obligation for the information to be shared, e.g. where a Court Order requires it, or where there is serious risk to someone's health and safety if the information is not shared e.g. where a child is considered to be at risk of harm. In such cases, a manager must be consulted before any information is shared.

The duty of confidentiality only applies to information from which it is possible to identify the person it relates to and not to anonymised data used for management information or statistical reports.

The Data Protection Act 1998 does not apply to the records of people who have died. However, the same principles apply to the records of deceased people and these records will therefore be treated with the same degree of confidentiality as those of living people.

3.2 Security of Information

In order to comply with the requirements of the Data Protection At 1998 and ensure that confidentiality is maintained, access to both electronic and paper records must be controlled in the following way:

- Paper case records must be stored in lockable filing systems. When a file is removed from the filing system, it is the responsibility of the Admin Team Manager in that Service area to ensure that there is a system in place that records the details of the person removing the file, including the name, role and reason for removal, when the file is to be returned and the method of transporting and securing the file. It is the responsibility of the person taking the file to ensure that the file is returned and that any delay or concern is reported in a timely way to an Group Manager;

- When a paper file is removed from the secure filing system, the member of staff that it has been released to is responsible for ensuring that the file is kept securely. If a file is taken out of the office at any time, the reason for this must be agreed with an Group Manager whose consent will be given in exceptional circumstances only. While the file is out of the office, it should be kept in a secure setting ensuring there is no inappropriate access to it;

- Access to electronic records will require the use of a password which will identify the access rights of the individual and determine the type of record they can access and the actions they can perform on that record;

- All members of staff must only access a computer system containing personal information using the password issued to them, and must log out of the system when they have finished using it;

- Members of staff must never divulge their password to anyone else or allow anyone else to use a computer system without first logging out themselves;

- Storing personal information about children and families is only permitted on approved shared electronic folders, and must not be stored on floppy disks, laptops or the hard drive of a desktop PC. The use of memory sticks or any similar portable storage device to store children and families information is not permitted under any circumstances. Encrypted memory sticks may be issued to staff for use in exceptional circumstances for information such as presentations or reports that do not include personal information about any child or family (see Use of Removable Media Procedure at the **Walsall Council website** for details);

- Any contractor for offsite storage must meet these requirements as a minimum;

- A laptop can only be used if it has been encrypted and is password protected which will be set up for individual workers by ICT Services. All laptops must be kept safely and securely if

taken out of the office and returned to the office the next working day (see Secure Remote Working – a reference guide at the **Walsall Council website**);

- **Under no circumstances** should staff use their personal home computers or laptops to record or store information about service users, children and families. The use of any portable storage device with personal home computers is strictly prohibited;
- All staff and managers must attend regular and relevant training regarding data protection. All staff must complete the appropriate e-learning modules available via the corporate intranet, and also access any updated information and procedures regarding data protection and freedom of information via the corporate intranet;
- Staff and managers should ensure that they are familiar with Walsall Council's acceptable use policy relating to the use of emails and the internet. Full details can be found in the Email & Internet Usage Policy at the **Walsall Council website**).

3.3 Sharing Data with Other Agencies

Sharing information promptly with others working with the same child is invariably the key to safeguarding the child's interests. Relevant information, therefore, about children must be shared with colleagues, other professionals or agencies that may have a role to play in their care.

However, the general principle is that information may only be shared on a "need to know" basis. For example:

- Where professionals are undertaking a Section 47 Enquiry in relation to a child;
- Where the police are investigating a criminal offence or require information to help them find a missing child;
- Where information is requested in the furtherance of any inquiry or tribunal, or for the purposes of a Serious Case Review;
- In such circumstances, the person to whom the information relates should be informed that records have been requested unless to do so would prejudice the purpose of the request;
- Any objections they have should be considered before responding to the person making the request;
- Where information or records are passed to others, it should be noted and confirmed in writing.

Information may also be disclosed to persons who have a statutory right of access to the information, for example:

- Where the Court directs that records be produced or a **Children's Guardian** is appointed;
- Court reports must not under any circumstances be shared with anyone not party to the proceedings without the express leave and permission of the Court;

- Where information is requested by Inspectors of a regulatory authority, e.g. Ofsted (who have specific statutory powers that permit access to records).

3.4 Consent

At the first point of contact with Children's Social Care, or as quickly as possible afterwards, children and their families will be advised as to how any information obtained about them will be used. The explanation given should include details of:

- Any organisations or individuals that Children's Social Care may need to share their personal information with;
- The type of information that may need to be shared;
- The reason why the information may need to be shared;
- Any likely consequences of sharing the information.

Once this explanation has been given, the child (depending on his/her age) and the parent will be asked to give their consent in writing to the sharing of their information with other agencies. The person giving consent must fully understand what is being consented to and any likely consequences of giving consent. The fact that consent has been given should be recorded on the electronic record system Mosaic or on the paper file as appropriate.

The only exceptions are:

- Where the circumstances of the point of contact are such that it would be inappropriate to request consent to share that information, e.g. where the child may be at risk of significant harm and there will be a risk of further harm if consent is sought. The public interest in child protection overrides the public interest in maintaining confidentiality and the law permits the disclosure of confidential information necessary to safeguard a child/children. In this case, the reasons for not seeking consent must be recorded on the child's case record, together with the arrangements for ensuring that the explanation is given at another time;
- Where the child and parent are considered to be incapable of giving informed consent.

Prior to responding to a request for personal information from another agency, all staff must first check whether one of the exceptions apply or whether the person concerned has given their consent to share the information in question with the person or agency requesting the information for the purpose that the request is being made; if so, then the information can be shared.

3.5 Secure methods of sharing information

When information is shared verbally, members of staff will ensure that confidentiality is maintained and that the rules regarding transferring information on a "need to know" basis are observed.

Where information is to be shared by telephone, the member of staff will ensure that the recipient is properly identified. Where the recipient has initiated the telephone call, the member of staff will request the recipient's telephone number (their organisation's reception or switchboard, not the recipient's direct or mobile number) and will 'phone them back.

Documents containing personal information sent by post will be marked "Personal and Confidential – to be opened by Addressee only", and will only be sent it if can be guaranteed that it will be opened by the person to whom it is addressed. The addressee will be informed of the date, time and means by which the documents have been sent and asked to confirm receipt.

Fax transfer will be avoided whenever possible. Where it is unavoidable, the following will apply:

- The recipient is telephoned to ensure that they are aware a confidential fax is about to be sent and to confirm that an identified individual will wait by the machine, collect the fax, deliver it and 'phone the sender to confirm receipt;
- When sensitive information is to be faxed, a "two fax" approach will be adopted. Personal details without identification will be sent on one fax and the identifiers will be sent separately;
- A log will be kept of all confidential faxes sent and received, giving details of sender and recipient, date and time of fax and a copy of the machine's log confirming status of the transmission.

Personal information about individuals will only be transferred by email to an email address external to Walsall Council if the email address is secure and information is encrypted (refer to Information Security Procedures and Email & Internet Usage Policy at the **Walsall Council website**).

3.6 Agreements on Information from Third Parties and Inter agency Information

Third parties will be advised that all information they provide about children and their families will be routinely shared with those concerned and will be attributed to them. The agreement to share, if given, will be recorded on the child's case record.

The expectation is that other agencies will always consent that information they share will be disclosed to the child or person confirmed. Where a third party states that they do not want the information to be shared or attributed to them, this will be recorded on the record and advice sought from the appropriate manager. Once a decision has been made, this will also be recorded and the third party informed both verbally and in writing of the action taken.

Where a member of the public who makes a referral in relation to a child wishes to remain anonymous.

3.7 Contracts with Providers

All contracts with providers must include a condition of expectation that case records will be maintained in line with the Data Protection Act 1998 and the principles of this policy. All new Contractual arrangements with suppliers of goods or services to the Council will contain confirmation that the suppliers comply with all appropriate information security policies and procedures.

4. Access to Records

4.1 The Right of Access

Under the Data Protection Act 1998 any living person, about whom Children's Social Care hold personal information, has a right to access that information.

Normally the right of access will mean providing the individual with a copy of their records. However, with the agreement of the individual, it may be that they are allowed, under supervision, to examine their records (whether electronic on Mosaic or on paper) and to say what documents they want copies of.

4.2 Request for Access

Requests by an individual for access to their records should be made in writing wherever possible. Assistance to write an application should be given as required.

All requests will be handled by the Information Governance Team. Where a valid request is received under the Data Protection Act, directly by a service or member of staff, it should be forwarded immediately to that team for processing. This does not preclude officers from dealing with day to day enquires or providing 'data subjects' with their own information as part of 'business as usual'.

The Council will take reasonable steps to confirm the identity of the requester. However the Council will not make this identification process unnecessarily onerous and in cases where the requester is already well known to the Council (e.g. an existing member of staff or a social care client with an active social worker) formal identification will not be sought.

All requests will be responded to as promptly as possible, and in any event no later than 40 calendar days. The requestor should be kept informed of any delays.

Where Children's Social Care do not hold any personal information about an individual who has made a request for access to their records, the individual concerned must be notified as soon as possible.

Individuals will not be charged for access to their records.

Request by, or on behalf of, a child

The right of access extends to children who understand what it means to exercise that right. Where a child makes a request for access to their records, Children's Social Care will have to decide if he/she has sufficient understanding to do so. In other words, does he/she understand the nature of the request? If so, then the request for access should be complied with;

If a child does not have sufficient understanding to make his/his request, a person with parental responsibility can make the request on the child's behalf. Where a person with parental responsibility applies on behalf of a child, Children's Social Care must be satisfied that the child lacks the capacity to make a valid application, or has capacity and has authorised the application;

If Children's Social Care considers that granting access to the person with parental responsibility is likely to result in serious harm to anyone including the child, a decision will have to be taken whether or not to refuse access. If the decision is made to refuse access to the information to the person with parental responsibility on the grounds that to do so would result in serious harm, the person acting on the child's behalf may make an application to the Court or Data Protection Commissioner for access.

Requests made through another person (an agent)

If a person has capacity and has appointed an agent, the agent can make a valid request for access on behalf of the person concerned. Agents should provide evidence of their authority and confirm their identity and relationship to the individual. Such evidence must be provided in writing. When an agent makes a request on behalf of a Data Subject, signed authorisation from the Data Subject will be required. The Council may still check directly with the Data Subject whether he or she is happy with the agent receiving the personal data and should highlight the implications of the request.

Any request received from an agent must be accompanied by signed Form of Authority permission from the Data Subject. No proof of identity for a Data Subject is required when the application comes from a professionally recognised agent such as a Solicitor.

Requests for access to the records of a deceased person

The Data Protection Act 1998 applies only to data about living persons. Data held on deceased persons, therefore, is not personal data as defined by the Act. Even though the Data Protection Act 1998 does not apply to such data, there may still be issues of confidentiality surrounding the rights of others to access records about the deceased. Advice should be sought from Legal Services where necessary.

4.3 Information to be Disclosed

All personal information held relating to the person requesting access to it should be made available to them, unless it is subject to any exemptions, or a third party has refused to consent to its disclosure. It should not be altered in order to make it acceptable to the person concerned.

The information to be made available to the individual must be that held at the time the request is received. Account may be taken of an amendment or deletion made between the time of the request and the supply, if the amendment or deletion is one which would have been made regardless of the request.

Information that includes details about another person

Where the information held about an individual also contains personal information about another person, all efforts must be made to provide as much of the information sought as can be disclosed without revealing the identity of the other person. There may be occasions, however, where it is reasonable in all circumstances to comply without consent. This includes the disclosure of identifiable details about a third party. In such circumstances, the authority of a manager is required before disclosure takes place.

Within the 40 day period (commencing from the date the request was received, or from the date further information was requested for the local authority to satisfy itself as to the identity of the person making the request) Children's Social Care must endeavour to seek the consent of the third party for the information held about them to be disclosed.

If such consent is not given by a third party within 40 days, Children's Social Care should give as much information as possible to the individual requesting access to their records, without identifying the third party. The applicant should be told why some of the information requested has not been given.

Where consent is not or cannot be given and Children's Social Care considers it reasonable to comply with the request without consent, then it may be required to justify its actions. In such circumstances, the authority of a manager is required before disclosure takes place.

Where Children's Social Care are satisfied that the individual requesting access to the information will not be able to identify the third party from the information, taking into account any other information which is likely to be in or come into the possession of the individual, then the information must be provided.

If full access is not given or the person requesting access believes that Children's Social Care has failed to comply with the request, then he/she can apply to the Information Commissioner or the courts.

Where the information an individual wishes to access includes information provided by a third party on the basis that it will remain confidential, every attempt must be made to obtain the consent of the third part for the information to be disclosed. Where consent cannot be obtained, a decision must be made as to whether the information should be shared or not. In reaching this decision, consideration should be given to:

- Any duty of confidentiality owed to that third party;
- Any steps taken with a view to seeking consent of the third party to the disclosure;
- Whether the third party is capable of giving consent;
- Any express refusal of **Consent** by the third party;
- The decision and the reasoning behind it must be recorded on the case record

4.4 Presenting the Information

The Data Protection Act 1998 requires the information to be communicated in an intelligible form, and that the individual requesting access should be provided with a permanent copy of the information. However, a copy need not be supplied if it is not possible, or would involve disproportionate effort, or the individual agrees otherwise.

Some of the information may already be known to the individual requesting access but it may still be helpful to have someone available to help him/her to understand the material or explain anything that he/she does not understand.

4.5 Exemptions from Access

The Council uses the presumption of release as the starting point for all valid subject access requests. Where there is a legitimate reason why information should not be disclosed (e.g. the prevention or detection of crime) the applicant will be informed of the reasons why and of their right to appeal. Exemption may be available in the following circumstances:

- For the purposes of the prevention or detection of crime, or to apprehend or prosecute offenders (Information will only be released where disclosure meets the criteria outlined in Section 29 of the Data Protection Act 1998. Requests under s29 will only be considered from an agency with a crime or law enforcement function, including the Police, HMRC, UK Visas and Immigration, or the Benefit Fraud sections of DWP or other Local Authorities);

- Where information about him/her has been disclosed to another organisation which required it for any of these purposes (e.g. the police);

- Where information has been received from an organisation which had it in its possession for any of these purposes;

- Where the provision of such information would be likely to prejudice disclosure or would be likely to prejudice any of these purposes.

In addition, where the offence involves any unlawful claim for a payment out of public funds (e.g. benefits), personal information is exempt from subject access to the extent to which such exemption applies in the interests of the operation of the system.

For the above exemption to apply there would have to be a substantial chance rather than a mere risk that the purposes would be noticeably damaged. As a result, Children's Social Care need not comply with a request from organisations requiring the information for any of these purposes, nor refuse subject access to such information unless it has been provided with sufficient information to enable it to judge whether or not prejudice is likely. Such requests should be treated on a case by case basis and use of the exemption should be the exception rather than the rule. Legal advice should be sought where doubt exists.

Personal information held for the purposes of social work is also exempt from these subject access provisions, where the disclosure would be likely to prejudice the carrying out of social work, by causing serious harm to the physical or mental health, or condition, of the person requesting access, or another person.

Access cannot be refused, however, where the existence of information would reveal the identity of a relevant person (e.g. a social worker) unless the serious harm test applies.

In making decisions on whether or not to give access to certain information, there is no general test of what constitutes a risk of serious harm. Decisions have to be made on a case by case basis. Restriction on the right of access should be exceptional and confined to serious harm, for instance where there is sufficient risk to the safety of a child for a **Child Protection Plan** to be in place and where disclosure would prejudice the plan. In some cases, access may have to be denied

permanently. In others, it may have to be deferred. The person seeking access may need special counselling during the period of deferment.

Information about physical or mental health or condition must not be disclosed without first consulting an appropriate health professional. This would normally be the person responsible for the person's current clinical care in connection with the matters to which the information relates. This might, for example, be a GP or psychiatrist.

Where other legislation prevents disclosure, then the individual requesting access cannot rely on the Data Protection Act 1998 to seek access to records. These include, for example, **Adoption Case Records**.

Local authority staff and elected members can use the Data Protection Act 1998 to gain access to personal information about themselves, if they have been in receipt of a service and the information is held for this purpose.

Access can be refused if an identical or similar request from the same individual has previously been complied with, unless a reasonable interval has elapsed between compliance with the one and receipt of the subsequent request. In deciding what amounts to a reasonable interval, the following factors should be considered:

- The nature of the information;
- The purpose for which the information is processed;
- The frequency with which the information is altered.

4.6 Where Children's Social Care Decide to Refuse Access

Any notification of refusal to disclose personal information should be given as soon as practicable and in writing, even if the decision has also been given in person. A record should be kept of the reason for the decision and this should be explained to the person concerned.

If a decision is made not to disclose some or all of the personal information, the applicant must be told the reasons, distinguishing between reliance on an exemption, inability to obtain consent of a third party or their refusal to consent.

4.7 Information that the Data Subject Considers to be Inaccurate

If a person considers that the personal information is inaccurate in any way, he/she can take the following action:

- Ask for the information to be corrected;
- Approach the Information Commissioner if he/she considers the information has not been appropriately corrected;
- Apply to the courts for an order requiring the information to be corrected, deleted or erased.

Children's Social Care may be required to correct information judged by the Information Commissioner or courts to be inaccurate and/or inform other organisations that may have received the information of the correction.

The person concerned may also be entitled to compensation for any damage suffered as a result of the use of information requiring rectification.

"Inaccurate" means incorrect or misleading as to any matter of fact. A mere opinion need not be corrected or erased, unless it appears to have been based on an inaccurate fact.

If Children's Social Care does not agree that the information is inaccurate, it should note in the record that the person concerned regards the information as inaccurate.

Requests for data to be corrected should be dealt with promptly, to avoid court action or intervention by the Commissioner, which may result. The local authority will also send a copy of the corrected data to the subject. The data subject should be notified within 21 days of action taken.

4.8 Challenge to Children's Social Care's decision to refuse access or amend records

If disclosure is refused by Children's Social Care, the person requesting access may appeal against that refusal either to the Information Commissioner or the courts. It is for the person concerned to decide which appeal route to take. The court has the power to order disclosure or to order correction or erasure or to confirm non-disclosure.

The Information Commissioner may issue enforcement notices for a breach of the Data Protection Act and its principles but only if the Commissioner is satisfied that a contravention has taken or is taking place.

Appeal by Children's Social Care again enforcement notices to Data Protection Tribunal:

- There is a right of appeal to the Data Protection Tribunal against an enforcement notice. The notice may be cancelled or varied in certain circumstances.

5. Complaints / Appeals

The Council has an Appeal Procedure for dealing with complaints. Any person who is unhappy with the way in which the Council has handled their request may use this procedure. The Information Commissioner is unlikely to investigate any complaint about the Council's handling of an information request unless the complaints procedure has been exhausted.

Appeals will be heard by an officer(s) not involved in the original decision.

A complaint may be made about the Council's failure to release information in accordance with its Publication Scheme, failure to comply with an objection to processing or to amend inaccurate records. Individuals have the right to rectify records and where they have accessed their record and identified information that they feel is inaccurate or irrelevant, they have the right to request that the information is altered or erased. Where Children's Social Care refuse to amend the record, the service user has the right to appeal.

Complaints can also be made about requests that have not been properly handled, or where there is dissatisfaction with the outcome of a request.

Appeals against denial of access to records (whether total or partial) should be made via the Tell Us Procedure which deals with the complaints process (see Tell Us Procedure Manual at **Walsall Council website**).

6. Documents to be Routinely Sent to Service Users

Records of assessments, which clearly identify aims, needs and outcomes achieved as well as identifying unmet needs, will be routinely copied to the subject of the assessment.

7. Public Information on Policy and Practice

All reasonable steps will be taken to publicise the open access policy and the rights of services users throughout the community.

All publicity will be produced in various formats as well as in a range of languages.

Posters will be displayed within Council offices, units and other public places.

8. Management of the Policy

This policy document has been approved by Children's Specialist Services.

Managers are responsible for the implementation of this policy and the appropriate procedure for monitoring, auditing and maintaining standards of which will be overseen in supervision in accordance with Supervision Standards.

Each Service area will comply with the audit and monitoring requirements of the over- arching Quality Assurance Framework.

Appendix 1: Eight Principles of the Data Protection Act 1998

Walsall Council is fully committed to the eight main principles of the Data Protection Act 1998.

When collecting and processing personal data the following principles will be applied:

- **Personal data shall be processed fairly, lawfully and, in particular, shall not be processed unless specific conditions are met**:
  The council will ensure that the collection and processing of information is not excessive and that it is appropriate to fulfil the operational needs of the organisation or to comply with any legal requirements.

- **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those**

purposes:
The council will ensure that when information is collected, on forms or by other methods, specific advice is given as to the purpose(s) of gathering and using the information.

- **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed**:
  The council will ensure the quality and accuracy of any information used and that any information held is factually relevant to the area of work concerned.

- **Personal data shall be accurate and, where necessary, kept up to date**:
  The council will endeavour to ensure that any personal data is accurate and current and where discrepancies are found, the data will be amended.

- **Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes**:
  The council will ensure that any personal information is not held for longer than required and, by applying checks to determine the length of time information is held, make sure that personal data is destroyed in an appropriate manner once the retention period has expired.

- **Personal data shall be processed in accordance with the rights of data subjects under the Act**:
  The council will ensure that an effective process exists to allow data subjects to fully exercise their rights to request to see any of the information held about them within the authority and to ensure that any such request is responded to within the legal time scale of 40 calendar days.

- **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data**:
  The council will ensure that appropriate procedures are in place to safeguard personal information and ensure that access is restricted only to those council officers who require it.

- **Personal data shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**:
  Walsall Council will ensure that personal information is not transferred abroad without suitable safeguards.