Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

Data Protection Policy including Subject Access Request and Safe Haven Procedures

Document Information					
Board Library Reference	Document Type	Document Subject	Original Document Author	Assured By	Review Cycle
GOV_IGCM_01	Policy and Procedure	Data Protection	Information Governance Manager	Trust Board	3 Years

Version Tracking				
Version	Date	Revision Description	Editor	Approval Status
1.0	21/02/2005	Approved on behalf of the Board by the IM&TSG	Information Governance Manager	Approved
1.1	20/11/2007	Reviewed for accuracy and addition of Subject Access Request and Safe Haven Procedures	Information Governance Manager	Draft
1.2	29/01/2008	Formatted to new Trust standard and renamed to reflect Integrated Governance Forum of origin.	Information Governance Manager	Draft
1.3	08/02/2008	Incorporated Modernisation & Workforce Integrated Governance Committee comments	Information Governance Manager	Draft
1.3	03/03/2008	Policy assured at Workforce and Modernisation	Information Governance Manager	Draft
1.3	04/03/2008	Policy assured at Integrated Governance Committee	Information Governance Manager	Draft
1.3	26/03/2008	Approved by the Board of Directors	Information Governance Manager	Approved
2.0	27/03/2008	Published	Information Governance Manager	Approved
2.01	06/11/2009	Complaints procedure updated	Information Governance	Draft

			Manager	
3.00	6/11/2009	Published	Information Governance Manager	Approved
3.01	11/11/2010	Administrative update	Information Governance Manager	Draft
4.00	21/01/2011	Reviewed by Information Governance Management Group	Executive Director of Finance and Commerce	Approved

Table of Contents

1. Introduction

Avon and Wiltshire Mental Health Partnership NHS Trust (AWP) is bound by the provisions of a considerable number of items of legislation and regulation affecting the stewardship of personal data.

The AWP Overarching Information Governance Policy defines the Trust's mandated approach for compliance and effective management in each of the following six areas of Information Governance.

- Information Governance Assurance
- Confidentiality & Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

Each of these six areas has a discreet and detailed policy and associated procedures which collectively constitute the top level documentation of the Trust's Information Governance Management System (IGMS).

2. Purpose

This document sets out AWP's policy for addressing its legal obligation to comply with the Data Protection Act of 1998 (DPA) which enshrines citizens' rights to the privacy and confidentiality of information about them that is held or processed by the Trust (in support of Article 8 of the Human Rights Act of 1998, the "right to respect for private and family life").

3. Scope

This Policy applies to Personal Data (staff, service user and other data subject information) that is either held or processed by the Trust across all Directorates and Strategic Business Units.

4. Roles and Responsibilities

4.1. The Chief Executive

The Chief Executive is accountable for the Trust's compliance with all applicable legislation and regulation, including those described in this policy and associated procedures.

4.2. Directors of Strategic Business Units

Service and Clinical Directors of Strategic Business Units (SBUs) are jointly and severally responsible for the implementation of this policy and associated procedures uniformly across administrative and clinical functions within their Strategic Business Units.

4.3. Executive Directors

Executive Directors are responsible for the implementation of this policy and associated procedures across their Directorates.

4.4. The Caldicott Guardian

The Caldicott Guardian is responsible for championing the principles of Data Protection and Confidentiality across the Trust.

4.5. The Information Governance Manager

The Information Governance Manager is responsible for the maintenance and review of this policy and associated procedures.

4.6. The Data Protection Officer

The Information Governance Manager, who is also the Trust's Data Protection Officer, is responsible for:

- Maintaining Information Commissioner notifications
- Facilitating Data Protection and Confidentiality training across the Trust
- Co-ordinating the administration of subject access requests
- Acting as the initial point of contact for any data protection issues which may arise within the Trust
- Recording any Data Protection and Information Security incidents which constitute breaches of Trust policy

4.7. The Information Technology Security Specialist

The Information Technology Security Specialist is responsible for achieving compliance with NHS and legal standards of information technology security, across the organisation, with particular emphasis on technical data protection issues.

4.8. Individual Staff

All Trust staff and those working on behalf of the Trust in any capacity that work with e.g. have access to personal data are required to adhere to this policy and to follow the associated procedures where appropriate.

4.9. Expert Advice

Expert advice in support of this policy will be provided by the Information Governance Manager and the Caldicott Guardian.

5. Policy Statement

All Personal Data held or processed by the Trust, either as the Data Controller, will be held and processed in accordance with the requirements of the Data Protection Act 1998 (the Act).

The "Eight Principles" of the Act are:

Personal Information about living people must be processed fairly and lawfully, and must:

1) Only be processed in accordance with the Act (or not processed at all),
2) Only be processed for a recognised legal purpose,
3) Be adequate for, and proportionate to the purpose,

4) Be correct (accurate and up to date),
5) Be kept only long enough to achieve the stated purpose,
6) Be processed in accordance with the data subject's rights,
7) Be processed and handled safely and securely,
8) Not be sent outside of the EEA (European Economic Area) unless that country ensures adequate level of protection of the data subjects in relation to the processing of the data.

All Personal Data held or processed by the Trust as a Data Processor, will be held and processed in accordance with the seventh principle of the DPA which states that personal data must be processed and handled safely and securely,

5.1. Policy Principles

The principles of this Data Protection Policy are:

The Trust will implement appropriate organisational and technical measures to ensure that:

- Personal Data processed by the Trust is treated in accordance with the requirements of the Data Protection Act 1998, in order to ensure that:
    - Data Subjects' rights in terms of Article 8 of the Human Rights Act of 1998, the right to "respect for private and family life", are upheld across all flows of Personal Data in the Trust's control,
- Planning of organisational and service activity will be undertaken in conjunction with a formal Privacy Impact Assessment to determine appropriate, effective and affordable Data Protection controls, and to implement them across the
- The quality and integrity of recorded Personal Data will be developed and maintained to ensure that it is fit for the purposes for which it was collected,
- Compliance with the regulatory framework will be audited, monitored and maintained.

6. Definitions

The following terms are used in the Data Protection Act 1998 and this policy, with specific meanings as described:

6.1. Data

Section 1(1) of the 1998 Data Protection Act defines 'data' as:

Information which -

a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose,
b) Is recorded with the intention that it should be processed by means of such equipment,

c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

d) Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record, or

e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

6.2. Relevant Filing System

A relevant 'filing system' is defined in (s.1(1)) as:

'Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.'

6.3. Accessible Records

Paragraph (d) of the definition of 'data' includes accessible records. Section 68 of the Act defines accessible records as a health record, and educational record or an accessible public record. In the context of this policy, the terms "information" and "data" refer to any item of personal data about living individuals, held in "accessible records" including manual files, computer databases, videos and other automated media, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, prescriptions, photographs, x-rays, scans and even telephone recordings.

6.4. Data Subject

A 'data subject' is defined as any individual who can be identified using the information or data held, i.e. the "subject" of the data, or from combinations of the data and other information which the data Controller has, or is likely to have in future.

6.5. Personal Data

'Personal Data' is defined in schedule 1(1) as:

a) data which relate to a living individual who can be identified —

b) from those data, or

c) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Personal Data includes:

'data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual'.

6.6. Sensitive Personal Data

'Sensitive Personal Data' is defined in schedule 2 as personal data relating to any one or more of the following:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs of a similar nature
- Trades Union membership
- Physical or mental health conditions
- Sexual life
- The commission or alleged commission by the data subject of any offence
- Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

Data Controllers are forbidden from processing sensitive personal data unless one or more of 19 specified conditions are met. These conditions are:

- Explicit consent
- Employment law obligations
- Vital interests of the data subject
- Not-for-profit organisation existing for political, philosophical, religious or trade union purposes
- Information made public by the data subject
- Legal rights
- Public functions (administration of justice, etc.)
- Medical purposes
- Records on racial equality
- Unlawful activity detection
- Protection of the public
- Public interest disclosure
- Confidential counselling
- Insurance and pensions – family data
- Insurance and pensions – processing
- Religion and health – equality or opportunity
- Political opinions
- Research
- Police processing

6.7. Data Controller

A ‘data controller’ is a ‘person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed’ (s. 1(1)).

6.8. Processing

‘Processing’, in relation to information or data, means:

a) obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —

b) organisation, adaptation or alteration of the information or data,

c) retrieval, consultation or use of the information or data,

d) disclosure of the information or data by transmission, dissemination or otherwise making available, or

e) alignment, combination, blocking, erasure or destruction of the information or data.

This definition of ‘processing’ is so broad as to include, for all practical purposes, anything that is done with information, including simply calling it up on a computer screen, reading a manual file, moving information over a network, email or on a portable memory device, and even includes recording of CCTV images and telephone recordings.

6.9. Notification

The Trust is required by the Act to ‘notify’ the Information Commissioner of all processing that takes place within the organisation, including each class of information processed, and the purpose for which it is processed.

Any changes to the classes of information processed, or the reasons for processing must be registered with the Information Commissioner by the Data Protection Officer.

7. Service User Information

All service users must be provided with information on the use and disclosure of confidential information about them that is held by the Trust. Staff should make sure that information leaflets on patient confidentiality and information disclosure are available in a format that is understandable to the service user, and staff should check, where practicable, that service users have read and understood the leaflets.

Staff should make clear to service users, in a way that is appropriate to that individual, when information is recorded and under what circumstances the health record will be accessed.

Staff must check that patients are aware of the choices available to them and that they have the right to choose whether or not to agree to information that they have provided in confidence being shared. Staff should communicate effectively with service users to ensure they understand what the implications may be if they choose to restrict the disclosure of certain information.

Leaflets and posters for service user can be found on the leaflets page on the Information Governance pages of Ourspace

8. Security of Staff and Service User Information

All staff and service user information, whether it is held manually or in an automated system, will be kept secure in accordance with the Trust's Records Management and Information Security Policies.

9. Sharing and Disclosure of Service User Information

All Data Controllers wishing to participate in information sharing agreements with AWP will be required to sign up to the most recent version of the Information Sharing Principles Agreement produced by the Avon IM&T Consortium in conjunction with organisations in the NHS, Social Services and partner organisations. This agreement is to be supported by "second tier" Information Sharing Protocols (produced by AWP) for each flow of personal data.

These second tier agreements will describe the data sets to be shared, the mechanism for sharing, and the roles of the originating and receiving Data Controller. To avoid confusion, they will not contain further descriptions of the Data Protection Act or the principles of information sharing. AWP will host a secure file sharing portal for managing all bulk flows of personal data between the parties described in the second tier information sharing protocols. AWP will not support the exchange of bulk transfers of personal data on other forms of media, including, for example, CD, DVD or paper.

10. Subject Access Requests

Section seven (7) of the Act allows an individual to:

Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

And if is the case to, to be given by the data controller a description of:

- The personal data of which that individual is the data subject
- The purposes for which they are being or are to be processed and,
- The recipients or classes of recipients to whom they are or may be disclosed
- To have communicated to him in an intelligible form:
- The information constituting any personal data of which that individual is the data subject
- And any information available to the data controller as to the sources of those data

Service User can obtain this information from the Trust by making a written request. This is known as a 'Subject Access Request'. The Trust's approach to dealing with Subject Access Requests by service users or staff is detailed in the Subject Access Request Procedure, attached as Appendix A to this document.

10.1. Third Party Information

Where the Trust cannot comply with a subject access request without disclosing information relating to another individual who can be identified from that information, the Trust is not obliged to comply with the request unless -

- the other individual has consented to the disclosure of the information to the person making the request, or
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

10.2. Staff Information

All staff information will be handled in accordance with the DPA in terms of its collection, processing, storage, retention and disposal. Any member of staff current, past or potential (applicant) who wishes to have a copy of their information under the Subject Access provisions of the DPA may submit a Subject Access Request to the Data Protection Officer.

11. Staff Training

The Trust will provide appropriate training and awareness programs to ensure staff are aware of their responsibilities for Data Protection, Confidentiality and Information Security. These awareness initiatives will be included in the Trust's Core Induction programme, and will be presented by the Caldicott Guardian or the Information Governance Manager.

11.1. Induction Training

The Induction Training program for Information Governance shall include:

- personal responsibilities
- confidentiality of personal information
- relevant Trust Policies and Procedures
- principles of the Data Protection Act
- individuals' rights of access to information
- general good practice guidelines covering security and confidentiality
- awareness of where to seek advice and support on matters concerning Data Protection, Confidentiality and Information Security

All new starters at the Trust will be required to attend mandatory Information Governance training as part of the Trust induction process.

A register will be maintained of all staff attendance at induction and other training sessions.

11.2. Specialist Training

Additional specialist training such as Information Security for System Managers may be provided for those with job functions that include responsibility for specialist areas such as system or workgroup managers.

11.3. Information Governance Training Tool

All staff are encourage to undertake the Information Governance Training modules that have been allocated to them within the Information Governance Training Tool.

12. Contracts of Employment

The Human Resources Directorate is to ensure that all staff have valid contracts of employment which will include specific clauses for Data Protection and Confidentiality.

13. Disciplinary Procedures and Enforcement

Breaches of this Data Protection Policy will be addressed through the Trust's Disciplinary Procedures. A copy of these procedures is available from the Board Policy Library on SharePoint.

14. Standards

This policy and related procedures or protocols will be assessed in terms of the standards defined in the Data Protection Act of 1998, and the Department of Health publication - Confidentiality: NHS Code of Practice.

15. Related Policy Documents

This Policy should be read in conjunction with the following IG Policies:

- AWP Overarching Information Governance Policy
- AWP Information Security Policy
- AWP Health & Social Care Records Policy
- AWP Records Management Policy
- AWP Freedom of Information Policy

16. Monitoring

This policy will be monitored and audited by the Information Governance Manager in accordance with the requirements stated in the Overarching Information Governance Policy.

17. References

17.1. References and Legal Framework

In addition to the Data Protection Act 1998, the legislation listed below also refers to issues of security and or confidentiality of Personal Data:

17.2. Data Protection Act 1998

17.3. Freedom of Information Act 2000

17.4. Computer Misuse Act 1990

17.5. Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)

17.6. Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992

17.7. Crime & Disorder Act 1998

17.8. The Directive on Privacy and Electronic Communications (2002/58/EC)

17.9. Electronic Communications Act 2000

17.10. Regulation of Investigatory Powers Act 2000

17.11. Lawful Business Practice Regulations 2000

17.12. Criminal Justice & Court Services Act 2000 (where Multi Agency Public Protection Panels & Information exchange is set out)

17.13. A full list of legislation can be reviewed within the NHS Information Governance Guidance on Legal and Professional Obligations at the following link:
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616

17.14. Additionally, the NHS has mandated a number of relevant regulations including:

17.15. Connecting for Health's Information Governance Toolkit

17.16. The Caldicott Report 1998

17.17. The International Standards Organisation Standard for Information Security Management,

17.18. Data Quality Assurance to include NHS Data Dictionary, Hospital Episode Statistics (HES) and Mental Health Minimum Data Set (MHMDS)

17.19. Confidentiality: NHS Code of Practice

17.20. NHS Records Management: Code of Practice

17.21. Information Security Management: NHS Code of Practice

17.22. BS10012:2009 Data Protection: Specification for a Personal Information Management System

17.23. The Care Record Guarantee

18. Appendix "A": Subject Access Request Procedure

18.1. Summary of Procedure

Data Subjects (people about whom the Trust holds Personal Data records) are entitled to request to see and obtain copies of these records.

A request from a Data Subject to a Data Controller to see such records is known as a Subject Access Request.

In general, Subject Access Requests are to be processed in accordance with the Data Protection Act 1998, within 40 working days of receipt of the request. The NHS aspires to a standard of 21 working days.

This document describes the process for dealing with Subject Access Requests, including what was formerly known as "Access to Health Records". Requests for access to health records relating to the deceased will continue to be made under the Access to Health Records Act 1990.

This procedure applies to Subject Access Requests by service users, staff or other Data Subjects wishing to obtain access to the data held by the Trust about them.

18.2. Informal Access Request by a Service User

Practitioners can share their own professional information with the service user. They may also withhold access to information if they believe it could lead to serious mental or physical harm to the service user or another person.

They must not disclose information that identifies another person ("third party") without their consent.

If the service user asks for information to be corrected, they should refer to guidance on corrections in section 17.10.

They must not disclose information recorded by another practitioner unless that practitioner has agreed to the disclosure. Any request for informal access that would involve such information should be treated as a formal access request. The practitioner should assist the service user in putting their request in writing, if required.

18.3. Responsibility for Processing Formal Subject Access Requests (SARs)

18.3.1. Service User SARs

Service Users may submit a SAR using the SAR form provided by the Trust. This may be submitted to any member of the Trust, but should ideally be submitted to a member of the clinical Team they receive care from.

Staff receiving a SAR from a service user are required to do the following:

- Ensure that the standard Trust SAR Form is completed, identification and proof of address is provided.
- Provide the completed SAR Form to the local Health and Social Care Records representative for processing.

- The local Health and Social Care Records representative is to acknowledge receipt of the SAR using the standard Trust letter.
- The local Health and Social Care Records representative is to follow the remaining SAR process as detailed below in section 17.4.

18.3.2. Subject Access Requests by Staff and others

Staff and other Data Subjects may submit a SAR using the SAR form provided by the Trust. This may be submitted to any member of the Trust, but should ideally be submitted to a member of the Human Resources Directorate or the Information Governance Manager.

Staff receiving a SAR from a service user are required to do the following:

- Ensure that the standard Trust SAR Form is completed, identification and proof of address is provided.
- Provide the completed SAR Form to the local Human Resources representative or the Information Governance Manager.
- The Information Governance Manager is to acknowledge receipt of the SAR using the standard Trust letter.
- The Information Governance Manager is to follow the remaining SAR process as detailed below in section 17.4.

18.4. Receipt of Requests

If a request is made via personal letter, then the Data Subject Access form and covering letter should be sent to the applicant for completion. Once received the following steps should be followed:

- The Acknowledgement Letter must be sent which advises the applicant that a fee may be payable in relation to the request.
- Check MARACIS or RiO as appropriate for hospital/NHS numbers and site indicator to establish location of records. If the site indicator does not record the location of the records, contact the last practitioner involved in the service users care.
- The records should be retrieved from records stores or archives and MARACIS or RiO as appropriate. The records should be reviewed to establish if a charge should be incurred in accordance with the charges set out in section 17.7.
- If a charge is to be levied the standard Receipt and Return of ID and Fees Letter should be sent to the applicant by recorded delivery only.
- The consultant or other lead practitioner must be identified.
- The records must be sent to the consultant or lead practitioner in a safe and secure manner.
- They must include the standard Professional Scrutiny Letter and the Granting Access to Health Records Form Note that, in law, only a health (not social care) practitioner can fulfil this responsibility for health records.
- Monitor the progress of the request, ensuring that the request is responded to promptly.

- All details regarding the request must be entered into the Subject Access Database.

18.5. Responsibilities of the Consultant and Lead Practitioner

On receipt of the health records, the practitioner should:

- Identify information that should not be disclosed under either the “serious harm” or “third party” provisions. Please refer to section 17.9.2.
- Provide an explanation of any codes or abbreviations that are likely to be unintelligible to the recipient.
- If the request is to view (not receive a copy of) the health and social care record, the practitioner should say who will undertake the supervised viewing in order for the service user to be contacted and an appointment made.

18.6. Responsibilities of Local Health & Social Care Records Representative

On receipt of the response from the practitioner, the records clerk/manager should:

- Consult the Caldicott Guardian/Information Governance Manager if denying access is being considered.
- Notify the Caldicott Guardian/Information Governance Manager in writing of the reasons why access is being denied, with details of the withheld information.
- If appropriate, contact any third parties requesting permission to disclose using the standard Third Party Consent Letter and await for response prior to disclosure.
- Ensure that the appropriate fee has been received prior to commencing photocopying.
- Ensure that those areas where access is not to be given are removed from the notes or excluded when photocopying.
- Make arrangements for copying or supervised viewing as appropriate.
- Update the Subject Access Database to reflect the current status of the request.

18.7. Supervised Viewing

The supervised viewing must not take place until the charge (if applicable) has been received.

A practitioner supervising a service user’s viewing of their records should answer any questions or refer the questions to another practitioner.

A non-practitioner supervising a service user’s viewing of their records should not seek to respond to questions relating to the content of the record, but should refer the matter to the relevant practitioner.

Update the Subject Access Database to reflect the current status of the request.

18.8. Sending Records to the Service User

The records can only be sent to the service user via recorded delivery as a minimum, and must be marked Private and Confidential - Addressee Only.

The Subject Access Database must be updated to reflect the current status of the request.

18.9. Non-disclosure

There are three provisions for non-disclosure.

18.9.1. Serious harm

Access can be denied if permitting access to the information would be likely to cause serious harm to the physical or mental health or condition of the service user or any other person (which may include a practitioner). For social care records, this provision is strictly that disclosure would *prejudice the carrying out of social work* by causing serious harm.

18.9.2. Third Party Information

The overriding rule is that the Trust should supply as much information as can be supplied without disclosing the identity of the third party. The identity is disclosed if the third party can be identified either from the information provided, or from that information and other information likely to be in the possession of the data subject. This does not apply if the third party is a practitioner involved in the care of the service user or where the third party has given permission for the service user to see that part of the record which concerns them.

18.9.3. Expectation of Disclosure

If a request for access is made by someone other than the service user, such as a parent for a child, there is a further provision for non-disclosure. Access can be refused if the service user had provided the information in the expectation that it would not be disclosed to the applicant, or had indicated that it should not be so disclosed. Access can also be refused if the information was obtained as the result of any examination or investigation to which the service user consented on the basis that information would not be so disclosed.

Access may no longer be denied on the grounds that the records were made before the introduction of the relevant legislation.

The advice of the Caldicott Guardian/Information Governance Manager should always be sought if denying access is being considered, including as to whether the service user should be informed that information has been withheld (as knowing that information has been withheld might itself cause serious harm).

Where access to health and social care records is denied, the Caldicott Guardian/Information Governance Manager must be informed in writing with a clear explanation of the reasons for denying access and a description of the information withheld.

18.10. Corrections to Records

Service users can ask for factual information to be corrected if it is inaccurate. The Trust must correct information that is factually incorrect.

A practitioner does not have to correct information that they believe to be accurate if a service user disagrees with it. They should make a note in the relevant part of the record of the matters alleged to be inaccurate, and should not delete entries.

In the event that a question of accuracy is taken to a court, the court can order that inaccurate information is rectified, blocked, erased or destroyed.

18.11. Special Conditions

Once the request has been received, no amendments to or deletions from the record must be made that would not otherwise have been made.

It is not necessary to comply with a request where an identical or similar request by the same individual has already been complied with, unless a reasonable period of time has elapsed. If you wish to take advantage of this condition, you should consult the Caldicott Guardian.

18.12. Applications from People other than Data Subjects

A number of other people are entitled to make requests for access to health and social care records, and certain special provisions apply. In other respects, the procedure to be followed is as above.

18.13. People Who May Apply for Access To Health and Social Care Records

The following people may apply for access to health and social care records:

- A named person who has the service user's written permission to do so, e.g. a solicitor, advocate or relative
- A person appointed by the courts to manage the service user's affairs.
- A named person acting *in loco parentis* for a child.
- A named person who has a claim arising from a deceased person's death.
- The personal representative of a deceased person.

18.14. Confirmation of Authority

The manager receiving the request should ensure that the appropriate written authority is received, such as consent from the service user or suitable legal documentation.

If a request is received from a solicitor enclosing a consent form for general release of health and social care records, it may be appropriate to contact the solicitor and/or service user to seek a clearer definition of which part of the records is expected to be released. Many solicitors investigating compensation claims for particular incidents under "no win, no fee" ask for a general consent form to be signed, and then seek release of all records, when the person concerned is under the impression that only records relevant to the incident are to be requested.

18.15. Claims and Compensation

If a request for access is known to be in relation to claims or compensation, the Information Governance Manager must be informed that access has been requested, and must be consulted. The Information Governance Manager will then liaise with the responsible manager in relation to the request.

18.16. Standard Letters

The following standard letters are to be used by the Trust for consistency in responding to SARs.

Standard letters include:

- Data Subject Access Application Form
- Acknowledgment Letter
- Requesting a Fee Letter
- Professional Scrutiny Letter
- Granting Access to Health Records From
- Disclosure of Records
- Non Disclosure of Records

18.17. Charging and Fees

The Trust is entitled to charge for SARs as follows:

- Solicitors - £50.00
- Services Users & Staff - £10.00 Administration Fee (£10.00 + 10p per double sided A4 sheet of photocopied notes)
- Recorded Delivery posting costs estimated on weight of photocopying.
- This charge must be itemised, and must not exceed £50.00 inclusive of all of the above.

Fees can be waived depending on the context of the request and the requestor's circumstances. Advice should be sought from the Health & Social Care Records when considering waiving fees.

18.18. Charges for Viewing Records

Records held entirely on computer - up to a maximum of £10 charge unless the records have been added to in the last 40 days, where there is no charge

Records held manually - up to a maximum of £10 charge unless the records have been added to in the last 40 days, where there is no charge.

Where the records are part held on computer and part manual - up to a maximum of £10 charge unless the records have been added to in the last 40 days, where there is no charge.

If the service user, staff member or other Data Subject viewed their records and then wanted copies, the £10 maximum charge for viewing would be included in the maximum £50 charge for copies. This would still be classed as one access request.

It has been agreed with the Head of the Exchequer that fees for access to records should be raised locally in order for the Health & Social Care Records Manager/Clerk to ensure payment is received prior to disclosure.

18.19. Complaints

Requestors who are dissatisfied with any element of the way their request is handled may write to the Chief Executive to request a review.

If, following a review by the Chief Executive, the requestor remains dissatisfied, they may apply directly to the Office of the Information Commissioner for a decision.

The Information Commissioner will not generally make a decision until the Trust's internal complaints procedure has been followed.

19. Appendix "B": Safe Haven Procedures

19.1. Introduction

The Trust Safe Haven Procedures set out requirements for best practice when transmitting Personal Data, to ensure the privacy and confidentiality of information in transit and at the point of receipt / delivery.

The term 'Safe Haven' was originally implemented to support contracting procedures. The Caldicott Report 1997 extended this concept to a term recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of personal data between organisations or sites.

This document will detail the procedures to be adopted when handling incoming and outgoing personal data by any of the following:

- Fax
- Post
- Email
- Telephone

19.2. Objectives of the Procedure

The key objectives of this procedure are:

- To ensure that all personal data is handled in accordance with the Caldicott Principles.
- Justify the purpose for using personal data.
- Only use personal data when absolutely necessary.
- Only use the minimum amount of personal data necessary.
- Access to personal data should be on a strict need to know basis.
- Everyone with access to personal data must be aware of their responsibilities.
- Everyone must understand and comply with the law.
- To ensure that the legal obligations of the Data Protection Act 1998 are adhered to.
- To provide a consistent approach to the way personal data is handled
- To provide guidance of the correct way to handle personal data.

19.3. Scope of this Procedure

This procedure applies to all employees of the Trust including permanent, temporary and contract employees, students, and volunteers, who come into contact with Personal Data. It applies equally to service user, staff and other Data Subjects.

19.4. Breaches of Confidentiality

All breaches of confidentiality must be reported whether they are the result of action taken by the Trust or a third party. These should normally be reported to your line manager, the Information Governance Manager and recorded on an Adverse Incident Report Form. If your line manager is unavailable then report the incident to the Information Governance Manager. What is personal data?

19.5. Personal Data can be any of the Items Listed Below

- Surname
- Forename
- Initials
- Address
- Date of Birth
- Postcode
- Gender
- Occupation
- Telephone Number
- Ethnic Group
- NHS Number
- National Insurance Number
- Local Identifier (e.g. hospital number)
- Other data (e.g. death, diagnosis)

19.6. Using Fax Communications

19.6.1. Physical Location

As far as possible a safe-haven must be established as a clearly identifiable part of the organisation's premises. Where particular healthcare functions are based in a number of locations, safe-haven procedures should apply to each location. Throughout the Trust there are a number of designated safe-haven areas. Senior managers must ensure safe haven areas are set up for sending and receiving faxes and postal information. Guidance can be sought from the Information Governance Manager. The requirement for additional fax equipment must be justified, taking into account the risks to personal data and the location of the machine. Details of the new equipment must be reported to the Information Governance Manager for inclusion in the list. Further guidance on the location of fax machines can be sought from the Information Governance Manager. Such areas must be physically secured as far as possible, that is, lockable and access to them should be restricted to those whose work requires it. Restriction to the area may take the form of card access, number pad and lock and key.

19.6.2. Outgoing Fax Communications

When sending a fax containing personal data it should be sent to a known Safe Haven fax machine. However it is appreciated that this is not always possible. In these cases additional steps will need to be taken to uphold the security of the information.

- Telephone the intended recipient of the fax to let them know that you are going to send a fax containing personal data.
- Ask the recipient to wait by the fax machine while the fax is sent.
- Ask the recipient to immediately acknowledge receipt of the fax.
- Ensure that the fax cover clearly states the intended recipients' names, does not identify the personal data and contains a confidentiality disclaimer. The standard AWP template that should be used by all staff is contained in the Safe Haven Procedures at Appendix C. A copy can be obtained from the Information Governance Manager.
- Double check the fax number before sending the fax.
- Use pre-programmable numbers for regular recipients.
- Request a report sheet to confirm the transmission was successful.

If you receive a request to fax personal identifiable to a new fax number then the Safe Haven External Request Form contained in the Safe Haven Procedures at appendix D, should be used to confirm the fax is indeed a Safe Haven fax.

Do not send a fax to a destination where you know it will not been seen for some time. Do not leave the fax machine unattended while the information is being transmitted.

19.6.3. Incoming faxes

Fax machines are located in various locations throughout AWP where transmissions will be received by staff. As with outgoing messages, incoming ones must also be subject to secure handling procedures.

- The intended recipient of the fax should be contact immediately a fax is received for them.
- Whilst awaiting collections, the fax should be placed away from public and other staff members view.
- If the fax is not collected the same day, it should be place in a sealed envelope, marked 'confidential' and sent to the intended recipient.
- Occasionally, confidential faxes will be received where the intended recipient is not clear. In these cases, they should be passed to a nominated person within leach location. It is suggested that a senior manager should assume this responsibility.

19.7. Postal Communications

19.7.1. Outgoing

Wherever possible, personal data should be sent through the internal mail system, delivered personally or collected in person.

If it is necessary to send personal data via mailing services, the following steps should be taken:

- Confirm the name, department and address of the intended recipient
- Ensure the contents of the letter cannot be seen through the envelope
- Ensure the envelope is properly sealed
- Mark the envelope 'Private and Confidential – to be opened by addressee only
- If appropriate, send the information by recorded delivery
- If appropriate request confirmation of receipt from the recipient

19.7.2. Incoming Post

Incoming mail should always be opened away from public areas. Under no circumstances should items addressed to an individual and marked 'Private and Confidential' be opened by the staff responsible for opening the Trust's post. They should be sent to the individuals Line Manager, or Personal Assistant as agreed between themselves.

Items marked to a department and an individual, should be passed to the Head or Manager of that department.

Items not marked with a name or department and are not labelled 'Private and Confidential' should be opened by the post staff to establish the intended recipient.

Any unmarked items that contain personal data should be placed in a sealed envelope and passed to the individual with responsibility for the Safe Haven.

19.8. Email Communications

19.8.1. Outgoing Personal Data

There are a number of risks of associated with sending personal data via email which must taken into account before deciding to use email as a means of communication:

- There is a risk that the email communication will not just remain with the personal data, as there is the ability for it to be forwarded to other users, as well as the risk of unauthorised disclosure.
- There is of course the increased risk that messages could be mistakenly transmitted to an unintended recipient.
- Person confidentiality may be breached. This could occur not only if the email is misdirected, but also if family and friends of

the person access the email from a shared computer. In addition, confidentiality may be breached if there is access to the clinician's email system by third parties such as, for example, clinical support staff.

- Risk also arises because there is often no way of guaranteeing that the personal data has picked up an email and is aware of its content. This is particularly significant pending on the urgency of the information communicated.
- In a similar context, there remains the very real risk that emails which are sent by patients will not be considered promptly by clinicians. This could result in urgent clinical communication being missed. Likewise emergency or urgent communication would not be distinguishable on the computer system. Consequently there would be an onus on clinicians to ensure that urgent emails are picked up promptly.

Consequently staff should take appropriate precautions if they intend to use this method of communication. This must include obtaining the person's consent to communicate in this way, and including a copy of this consent in the relevant record.

19.8.2. Email between staff about a Service User

Taking into account the risks documented above, personal data can only be sent from an AWP email account, to an AWP email account, for example:

xxxxxxxxx.xxxxxxx@xxx.xxx.xx to xxxxxxxxx.xxxxxxx@xxx.xxx.xx

or

from a NHS.net email account to an NHS.net email account, for example:

xxxx@xxx.xxx to xxxx@xxx.xxx

Third parties, e.g. organisations that have legitimate reasons to have access to personal data are able to request a third party nhs.net account.

Emails containing confidential information should be clearly marked 'Confidential' and the service user or staff member name should not be identified in the subject line of the email.

Advice can be obtained from the Information Governance Manager.

19.8.3. Email Disclaimer

The Trust does not have an approved email disclaimer nor does it recommend personal disclaimers are added by individuals. The use of a disclaimer will not offer any protection with regards to negligence either by the Trust or its staff. However all staff have a legal duty to protect all personal data confidentially. The duty to protect personal data confidentially applies irrespective of the form in which the data is transmitted.

19.8.4. Incoming Email

Although AWP has little control over emails received within the Trust, staff should still remain aware of the dangers of opening messages from unknown or untrusted sources. All staff are reminded that they must sign and adhere to the Acceptable Use Policy.

Emails containing personal data received in error, should be forwarded on to the correct location, if known, as soon as possible and deleted from the mailbox of the original receiver. The sender should be informed that the message has not reached its intended destination and has been deleted.

19.9. Telephone Communication

Personal data should not be discussed using a 'hands free' capability unless the phone is in a single user office or car, and no other persons are present.

When taking a telephone call, be aware that some types of information cannot be shared over the phone:

Information requested by the Police must not be given over the telephone. Specific information sharing protocols are in operation and requests for information must be made in writing using official police paperwork.

Requests for information made by the press or media must be forwarded to the Chief Executive of the Trust as documented within the Caldicott Guidance – Using and Sharing Service User Information.

The following steps should be taken when personal data is requested over the telephone:

- Confirm the name of the person making the request along with their job title, department and organisation (if applicable).
- Establish the reason for the request.
- Take a contact telephone number. This should be a main switchboard number not a mobile or direct line number.
- If you are in any doubt of the caller's identity, call them back preferably via a main switchboard if possible.
- If in doubt, check the information can be released and telephone the caller back.
- Provide the information only to the person making the request – do not leave a message either with somebody else or on an answering machine.

19.10. Speaking to Relatives or Next of Kin

When speaking to persons claiming to be relatives or next of kin of a service user, the service user should ideally speak directly to the caller, or staff should ask the service user what details they would like to divulge to the caller.

Always:

o Check identity of caller and data subject's full name.

- If in doubt, call back using a documented number.
- Or – allow service user to speak directly to the caller.
- Or – ask service user what they would like you to pass onto the caller.
- If unsure pass call to senior member of staff.

19.11. What Information Can you share with staff?

Staff have the right to relevant information in order to support their role in caring for the service user.

Check identity of the member of staff – name, department and nature of enquiry.

If you have to give clinical information, be aware of others who may be listening.

19.12. Providing Information to a GP Practice

Check the identity of the caller and the service user's full name, NHS and hospital numbers.

If in doubt, call back using documented GP Practice number.

If unsure pass call to senior member of staff.

19.13. What information can you give to Employers?

No information without documented consent from the service user.

19.14. Using the telephone to contact Service Users

If you think you may need to contact a service user by phone, ask if you can leave messages and ensure that you document this in the service user's health and social care records. If you need to contact the service user urgently and they are not available, please leave your name, telephone number and a brief message asking them to call you back.

DO NOT MENTION THE HOSPITAL OR LEAVE ANY CLINICAL INFORMATION

Unless you can guarantee that the message will be delivered to and received by the correct service user then do not leave a message.

19.15. Advice from Connecting for Health on leaving telephone messages

Unless one has the service user's consent to do so and can guarantee that the message will be delivered to and received by the correct service user, then confidentiality concerns suggest it is a route that should not be taken.

Doctors who wish to provide a telephone or on-line service should consider carefully whether such a service will serve their service user's interests, and if necessary, seek advise from their professional association or medical defence society.

20. Appendix "C": Fax Header Sheet

Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

To
Name
Address

From
Name
Address

Tel
Fax

Tel:
Fax:

Facsimile Transmission

Any transmission problems call on the phone number above

Urgent		Routine		Confidential		Number of Pages		Date	

CONFIDENTIALITY

This facsimile transmission is strictly confidential and intended solely for the addressee. It may contain information, which is covered by legal, professional or other privilege. If you are not the intended addressee, you must not disclose, copy or take any action in reliance on this facsimile and please dispose of it confidentially. If you have received this facsimile in error, please notify us as soon as possible.

Message:

DO NOT MENTION ANY PERSONAL INFORMATON ON THIS COVER SHEET

21. Appendix "D": Safe Haven External Fax Request for Information

Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

To
Name
Address

From
Name
Address

Tel
Fax

Tel:
Fax:

Facsimile Transmission

Any transmission problems call on the phone number above

Urgent		Routine		Confidential		Number of Pages		Date	

REQUEST TO RECEIVE PERSONAL DATA VIA FAX

Trust staff to complete

I/we (insert name/department etc) _____have been requested by (insert person and company etc_____) to fax sensitive personal data (as defined by the Data Protection Act 1998) to fax number (insert fax number _____).

In order to ensure that the information we send will be treated in accordance with the Data Protection Act 1998 and other relevant legislation, the Trust requires the following declaration is complete prior to commencement of the service.

Company/organisation to complete

I confirm that fax number (insert fax number) _____ is designated as a Safe Haven, i.e. it is in an area that is physically secure, lockable, with access restricted to those whose work requires it.

I confirm that any personal data received via the Safe Haven fax will be treated in accordance with the Data Protection Act 1998 principles and other relevant legislation to ensure confidentiality.

I confirm that should a breach of confidentiality arise it will be reported immediately to the Information Governance Manager for investigation.

Signature_____

Job Title_____

Telephone Number_____

Date_____