CONFIDENTIALITY

POLICY NO & CATEGORY	**IG 01**	**Information Governance**
VERSION NO & DATE	**2**	**August 2011**
RATIFYING COMMITTEE	**Clinical Governance Committee**	
DATE RATIFIED	**November 2011**	
NEXT REVIEW DATE	**September 2014**	
EXECUTIVE DIRECTOR	**Medical Director**	
POLICY LEAD	**Information Governance Lead**	
POLICY AUTHOR *(if different from above (Lead)*		
FORMULATED VIA	**Confidentiality and Data Protection Assurance Group** **Information Governance Steering Group**	

POLICY STATEMENT

Birmingham and Solihull Mental Health NHS Foundation Trust (BSMHFT) aims to maintain as confidential all personal information it collects and stores. The Trust will only obtain, record, store, use, disclose or delete personal information according to existing legislation and within the framework of the NHS Confidentiality Code of Practice.

KEY POLICY ISSUES

- All Staff to follow the NHS Confidentiality Code of Practice.
- The policy covers all personal identifiable information about service users, carers, staff and other persons that may have contact with the Trust.
- Data subjects must be given information on how information may be shared.
- Sharing confidential information with other organisations must be supported by an agreed Information Sharing Protocol.
- Access to and sharing of confidential information should be on a need to know / minimum basis.
- All breaches of confidentiality should be reported through the incident reporting process.

CONTENTS PAGE

1. INTRODUCTION

The Trust maintains many records containing personal information and therefore the duty of confidence and other legislation, especially the Data Protection Act1998 apply equally to these records (e.g. service user records, care records, staff records, supplier records, complaints records, incident forms etc.).

The Trust is committed to following the patient confidentiality model as described in the NHS Confidentiality Code of Practice:

- Protect - look after the patient's information;
- Inform – ensure that patients are aware of how their information is used
- Provide choice – allow patients to decide whether information can be disclosed or used in a particular way and,
- Improve – always look for better ways to protect, inform and provide choice.

1.1. Rationale

The Trust has a legal duty to all data subjects (individuals), e.g. service users, families and carers, staff and others in contact with the Trust, to protect their personal information, to inform them how that information is being used, to inform them of their rights to access this information and where appropriate to seek their consent before disclosing personal information to other parties. There are a number of exemptions exist that may mean the Trust is not required to seek consent for disclosure of confidential information in some cases; however these need to be agreed with the Legal Department or Information Governance Lead.

The Trust has a duty to ensure that all staff are aware of confidentiality issue and are able to deal with matters directly or have appropriate advice and guidance available to them.

This means ensuring that all personal information relating to individuals is processed lawfully, fairly and transparently, so that they:

- Understand the reason for collecting, storing and sharing personal information (processing).
- Give their consent for the use and disclosure of personal information (where applicable).
- Have confidence in the way the Trust handles personal information.
- Understand their rights, including the right to access information held about them or the right to give consent to others to access this information on their behalf.

1.2. Scope

This policy sets down required practice for all who are employed by or are under contract to BSMHFT concerning confidentiality personal information. It sets out principles, standards and practical arrangements for the protection and appropriate use of confidential personal information. Its key references are the Data Protection Act, The Caldicott Report and the Department of Health Guidance "Confidentiality: NHS Code of Practice" - November 2003.

This policy should be read alongside related Trust policies and procedures, in particular:

- Information Governance Strategy
- Information Security Policy

- Information Governance Assurance Policy
- Care Records Management Policy and Procedures
- Confidentiality Audit Guidelines
- Information systems and information asset owner guidelines
- Safe haven Procedures- Transferring information securely
- Child Protection Policy
- Missing Person
- Management of CCTV Systems
- Safeguarding Vulnerable Adults Policy
- The management of Serious Untoward Incidents
- Mental Capacity Act 2005 Policy
- Guidelines for disclosing information to the police

Records/ Information covered

This policy covers all records/ documents that contain personal or confidential information (e.g. Service User records; Staff records; Carer records; Complaint/ Compliment records; Incident records etc).

The Trust will also apply the duty of confidence to clinical records of deceased clients, as suggested by NHS guidance.

The storing, issuing and transferring of manual care records (or part thereof) comes under the responsibility of the Head of Care Records (see Care Records Management Policy and Procedures).

There are also a number of non-personal records that will need to be treated confidentially, e.g. commercially sensitive information must be kept confidential. All aspects surrounding commercial sensitivity and disclosure of such information must be discussed with appropriate staff.

1.3. Principles

The Trust will always respect the confidentiality of service users, families, carers, staff and other third parties and not disclose personal information without consent, unless legally obliged to do so, if there is an overriding public interest (e.g. to prevent a serious crime), or if there are good reasons to believe that failing to share the information would put someone at risk.

2. POLICY

2.1. Overview

The Trust is committed to the delivery of a first class confidential service that follows Caldicott principles. All staff must ensure that all service user information is processed fairly, lawfully and as transparently as possible. All Trust staff have responsibility to meet the confidentiality standards outlined in this policy in accordance with the standard terms and conditions of their employment.

Any breach of this Policy would jeopardise the confidentiality of service users and the security of clinical information, and would breach the Data Protection Act (1998).

Breaches will be reported as incidents, which will be investigated by the Information Governance Office and may lead to disciplinary action against staff or heavy penalties against the Trust by the Information Commissioner's Office.

Confidential information about service users can only be used for healthcare purposes and unless exceptional circumstances are present, can only be disclosed with the informed consent of the service user. Where the service user lacks capacity and unable to consent, information should only be disclosed in the service user's best interests. When in doubt, staff must seek guidance from the Caldicott Guardian or IG Lead.

The only exceptional areas for disclosure of information when the service user has capacity are when statute law requires us to do so, when there is a court order and when disclosure may be necessary in the public interest.

All requests to access records should be processed following the "Procedures for Trust Staff on How to Deal with Requests for Access to personal data according to the Data Protection Act (1998)"

All Trust staff must ensure they are up to date on their statutory and mandatory training requirements and are aware of their responsibilities.

2.2. Definitions

For clarity there are a number of terms the Trust will adopt in relation to Confidentiality. These are explained in section 11 of the policy.

2.3. Legal Framework and NHS Guidance

There are a range of statutory provisions which limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. The following legislation and national guidance is relevant when considering whether confidential information should be accessed and/or disclosed, and has been taken into account in the creation of this policy.

- Common Law of Confidentiality **
- Data Protection Act 1998 (DPA98) **
- Human Rights Act 1998 (HRA98) **
- Freedom of Information Act 2000 **
- Access to Health Records Act 1991
- Computer Misuse Act 1990 **
- Administrative Law **
- Caldicott Report 1997
- Confidentiality NHS Code of Practice 2003 **
- Confidentiality: Protecting and Providing Information (GMC 2004)

(Note: ** indicates that this legislation and guidance equally applies to service user records, staff records or records relating to third parties)

This policy is in line with best practice advice given by regulatory bodies to their registered health professionals (e.g. Royal College of Psychiatrists). It is re-enforced by the guidance on the need to protect confidentiality of patient information held on electronic systems which was issued jointly by the NHS, GMC and the Information Commissioner (Joint Guidance on use of IT Equipment and Access to Patient Data – DoH 25 April 2007). This states:

'No IT system can be immune to inappropriate use by individuals who have been authorised to use the system and to access data. It is important therefore that all those who are provided with such authorisation by virtue of their role in delivering or supporting the delivery of care, understand and meet the standards of behaviour that are required by law and professional codes'.

It concludes:

'The General Medical Council, Information Commissioner and the Department of Health have agreed this joint statement to ensure that all those who have access to patient information in the course of their work are clear about what is expected of them. The Department of Health has strongly supported the Information Commissioner's call for stronger penalties to apply where individuals obtain information unlawfully, and the law is to be changed to provide the possibility of a custodial sentence for those found guilty'.

2.4. The 8 Data Protection Principles

The 8 principles of the Data protection Act states that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes (e.g. Healthcare)
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept any longer than necessary
6. Processed in accordance with the rights of the data subject
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside European Economic Area without adequate protection

2.5. Caldicott Principles

(Concerned with Patient Information only) The 6 Caldicott Principles are:

1. Justify the purpose(s) of using confidential information (e.g. to support patient care)
2. Only use it when absolutely necessary
3. Use the minimum that is required (e.g. when sharing information)
4. Access should be restricted on a need-to-know basis (e.g. team involved in patient care only)
5. Everyone must understand his/her responsibilities (e.g. to maintain and protect patient confidentiality, only share if necessary)
6. Understand and comply with the law

3. CORPORATE PROCEDURE- ACHIEVING THE POLICY

3.1. General Responsibility for Confidentiality

All employees, contractors, temporary staff and volunteers are responsible for maintaining the confidentiality of information whilst working within the Trust and after they have left the Trust.

Staff must only access personal information (including service user or staff records) if they have a genuine 'need to know/ legitimate reason'. Unauthorised access or use of such information will be investigated and may lead to disciplinary action and could be actioned under the Data Protection Act.

Everyone working for the Trust should be aware of their responsibilities in order to comply with law. (Including the Caldicott Principles)

All staff must ensure they know of, understand and apply recommended practical measures to maintain confidentiality when obtaining, sharing, storing or disposing of personal information in different communication forms. The Trust has a number of procedures and guidance document for staff which are available on the Intranet.

This policy gives the main points that need to be considered by every member of staff in their day to day duties.

3.2. Training

The Trust will ensure that appropriate information and training is available to staff so that they are confident in dealing with confidentiality matters in their work environment. Basic Information Governance training is provided through the mandatory Trust Induction and is part of the trusts statutory and mandatory training programme, and more specific training can be requested via the Information Governance Lead.

3.3. Information Collection

As soon as an individual is accepted as either a potential service user or employee, manual and/ or electronic records will be created and personal information stored in these files. Trust employees are responsible for keeping these records accurate, up-to-date, and confidential and ensuring that they are not shared outside the Trust unless required to do so.

On initial contact with the Trust the service user must be given information, *orally* and in writing, explaining the Trust's requirement to keep records, how these may be shared and service users' rights to access their information (Trust Leaflet No 4 – Access to your Care Record, Your Records Are Safe With Us).

Care Coordinators/ Lead Clinicians must periodically discuss information recording and sharing with service users to confirm understanding, identify any issues and note if consent to share information is not given (we must record consent). All such discussions must be documented in clinical notes (see relevant part of CPA policy and guidance).

Some service users (e.g. employees, relatives of employees or professionals who may be in contact with the Trust in their professional capacity) may feel the need to ensure that their computer records are further protected from unauthorised access by requesting their details to be anonymised. Such requests need to go through the anonymisation procedure and be authorised by the Caldicott Guardian.

3.4. Secure Transfer of Personal Identifiable Information

All transfers of personal identifiable information both to and from third party organisations are subject to strict governance and technical security controls. All staff intending to undertake in-bound and/ or out-bound personal identifiable information transfers must ensure it complies with all Trust policies including the ICT Security Policy and Safe haven Guidelines.

Staff must consider:

a) what information is to be transferred
b) number of records,
c) purpose of transfer,
d) nature of recipient,
e) method of transfer,
f) physical and technical security measures proposed by the sender and the recipient,

3.5. Requests for access to information

Individuals, or an appointed representative, have a right to request a copy of the personal information we hold on them (e.g. staff records, clinical notes, complaints information etc.) under the Data Protection Act. We have a duty to check the validity of such requests and once confirmed are legally required to respond within 40 calendar days. Information on how to deal with such requests is detailed in the Information Governance **section on the Trust Intranet)**. In the first instance all such requests must be directed to the Information Governance Lead/ Head of Care Records.

Where a request to disclose personal information has been received and is considered appropriate, the decision to disclose, what to disclose and the reasons for this decision must be formally recorded. In the case of staff records, it is the responsibility of the appropriate HR lead and the team manager to review the personnel file and identify information that should not be disclosed before they are copied and issued.

Guidance is available to staff reviewing records on the Trust Intranet and the Trust process will ensure all actions are monitored and logged for evidential purposes. When a service user gives consent to disclose information about themselves, clinicians should make sure that the service user understands what will be disclosed, the reasons for the disclosure, the likely consequences and record this information in the clinical notes.

If it appears that a service user does not have the capacity to consent to the sharing of information, clinicians should carry out a formal assessment of capacity, recording this in the care records. If the test demonstrates a **lack of mental capacity** the clinician must ensure that nobody else has a right to make the decision (a donee of lasting power of attorney for welfare decisions or a Court of Protection appointed deputy). If there is nobody else authorised to make the decision for the service user, the clinician should make a decision in the service user's best interests and record this decision on the appropriate form and in the service user's contemporaneous notes (see Mental Capacity Act 2005 Policy (C20)).

3.6. Regular Sharing

The Trust must agree an Information Sharing Protocol with any partner organisation where it is anticipated that regular information sharing will be required. All protocols must be logged centrally with the Information Governance Lead, who should also review protocols prior to agreement.

The protocol will lay down the principles under which information can and should be shared, how the information will be shared (e.g. hard copy, electronic), security, and details of the information to be shared in line with legislation.

Staff being asked to release service user information must be familiar with the relevant protocol and only release the minimum information required to fulfill the obligation and meet the request, in line with the arrangements in the protocol.

Where an information sharing request is received from an agency with whom the Trust has no information sharing protocol the requests must be passed to the Information Governance Lead/ Head of Care Records. Information Governance will determine if there is a valid reason to disclose and acceptable conditions at the receiving organization, consulting with Clinicians. Any disclosure must only be made in line with this policy.

3.7. Disclosure without Consent

There are only three exceptional circumstances that disclosure without consent in patient with capacity may be justified. These are where:

- Statute law requires,
- There is a court order,
- Disclosure may be necessary in the public interest where a failure to disclose information may expose others to risk of death or serious harm.

The courts, including coroner's courts, some Tribunals and persons appointed to hold inquiries have legal powers to require disclosure of information that may be relevant to matters within their jurisdiction. This does not require the consent of the service user, whose records are to be disclosed. Such disclosures must be strictly in accordance with the terms of a court order and should only provide the required information to the bodies specified in the order.

Disclosures in the public interest may be necessary to prevent serious crime or risk of significant harm. Public interest is described as exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.

Serious crime can be defined as cases involving murder, manslaughter, rape, treason, kidnapping and child abuse and may all warrant disclosure of confidential information in the public interest. Significant harm to the security of the State or public order also falls within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

Any disclosure of information should be proportionate and limited to relevant details. Each case must be considered on its merits. In circumstances, where it is difficult to make a judgment, staff should contact the Information Governance Lead or seek legal or other specialist advice through Trust Legal Services.

3.8. Research and Audit

If information is required for medical research or audit, staff should always evaluate each project whether personal identifiable information is needed for such purposes.

Unless there is genuine justification, all personal identifiable information described in this policy should be taken out to anonymise the data for research purposes.

There may be exceptional circumstances, where the use of patient identifiable information in research outweighs issues of privacy for public good. The National Information Governance Board for Health and Social Care (NIGB) has been given the powers provided under Section 251 of the NHS Act (2006) (formerly Section 60 of the Health and Social Care Act 2001) in such circumstances. It is important to note that Section 251 permits the temporary setting aside of the common law duty of confidentiality but does not set aside the requirements of the Data Protection Act (1998).

If staff identifies a potential application of Section 251 of the NHS Act (2006) prior to ethical approval of a project, the case should be made to the Caldicott Guardian following the initial approval of the NIGB, who will assess each case individually and refuse or accept the initial decision by NIGB to disclose the required information for research without consent for the public good. If ethics approval has been given to a research project without a section 251 approval, the Caldicott Guardian must be notified of this decision in writing.

All research staff must keep personal identifiable information secure at all times.

Associated researchers should clarify in research proposals the arrangements to obtain permission to access clinical information. Once explicit consent is obtained, researchers can use clinical information to conduct research.

3.9. Information Storage

Appropriate security arrangements must be in place to ensure that files are protected from unauthorized access and disclosure and from loss and destruction (see ICT Security Policy and/ or Care Records Management Policy.

Storing information electronically means that access to this information could be more widely available (e.g. on every Trust PC with a connection to the patient system) and therefore additional safety measures will be put in place:

- every user requiring access to a patient system will be given a unique user id and password that must not be shared
- staff will be required to sign a network access agreement form in which they accept responsibility for confidentiality and information security while using Trust systems (additional requirements will be covered in the Trust Information Systems Security policy)
- staff will be required to read and accept a confidentiality agreement notice when logging into the Trust network and, where possible, to individual applications.

Only ICT approved and Trust issued electronic systems must be used to store personal confidential information (a list of approved electronic information systems is held by the ICT Department).

No non Trust issued external media is permitted to be attached to Trust equipment or used to transfer Trust information. Trust issued encrypted memory sticks can be requested from ICT.

Electronic systems must be password protected (in line with Trust standards) and must have a robust back-up and recovery strategy in place to ensure the ability to recover from unexpected data loss with minimal impact on the Trust business.

Manual confidential/ personal files or information must be locked away when not in use, e.g. locked filing cabinet, secure office.

3.10. Transferring Information Security

Where personal identifiable information is shared electronically safeguards must be put in place to ensure confidentiality is not compromised (e.g. use of NHS.net (secure email) or encryption). Further advice is given in the Information Systems Security Policy or by contacting the ICT Service Desk.

Where personal identifiable information is faxed this must only be done to a safe haven fax. Staff must check that the correct fax number is used, complete the Trust standard fax header identifying the intended recipient and confirm receipt.

When mailing (external or internal) printed confidential information (e.g. clinical notes, staff files etc.) staff must ensure that they are securely packed (e.g. in tamperproof, clearly addressed envelopes marked 'Confidential') and have the Trust Safe Haven return address, in case of non-delivery, so that the risk of losing files is minimised. Refer to the Care Records Management Policy for further information on transferring Care Records.

3.11. Disposing of Confidential Information

Disposal of any Trust records must be in accordance with the NHS Records Management Code of Practice and the Trusts Corporate Records Management Policy.

Where confidential information needs to be disposed of, care must be taken to ensure that it is destroyed safely such that confidentiality is not breached **(see Disposal Guidelines on Intranet).**

Disposal of confidential information on magnetic media (e.g. PC hard disk, CDs, DVDs, memory sticks) must follow Trust ICT Department procedures (see '**Disposal of PC' Guidelines on Intranet).**

3.12. Handling of Confidentiality Breaches/ Incidents

Any incident involving the actual or potential loss of personal and/ or confidential information, should be considered as serious and should be dealt with initially as a **Serious Incident** (see 'Management of Serious Untoward Incidents' policy) This can be downgraded to a lower level incident if deemed applicable at a later date.

Access to personal information (e.g. manual and electronic records) is recorded in audit files and is monitored. The Trust will use this information to carry out Information Governance audits or investigations where a breach of confidentiality is suspected.

All incidents and issues which may include a breach of confidentiality and/or information security must be recorded on the Trust IRIS form and reported to the Information Governance Lead in a timely manner.

Breaches will be reported to and reviewed by the IG Confidentiality and Data Protection Assurance Group, who will ensure that appropriate actions are taken to minimise the risk of such incidents re-occurring. Where appropriate, incidents will be raised at the Information Governance Steering Group (IGSG), chaired by the Senior Information Risk Owner (SIRO).

Nominated senior managers will formally investigate serious breaches and where appropriate use the Trust's Disciplinary Procedure.

Staff who breach their duty of confidentiality may be subject to disciplinary action which could lead to dismissal.

3.13. Access/ Sharing of Confidential Information

Staff will be required to read and accept an ICT acceptance screen when logging on to the Trust network; which includes confidentiality; and, where possible, to individual applications as well.

In order to protect confidentiality:

- Service user information must not be disclosed under any circumstances for the purposes of fund raising or commercial marketing, although the Trust or its agents may do so with explicit consent from the service user.

- Care should be taken that images of Trust sites and services (e.g. photos, videos etc) do not identify service users or staff members without their permission.
- Although there is no legal obligation under Data Protection to keep personal information confidential after the death of a person there is an ethical obligation for NHS organisations to do so (see NHS Confidentiality Code of Practice). Information about a deceased person should only be passed on with the consent of their executor (such as next of kin, solicitor or someone with written confirmation that they are administering the deceased estate). Access request to health records for a deceased person can also be made under the Access to Health Records Act 1990.

4. ROLES AND RESPONSIBILITIES

This policy applies to permanent and temporary staff, students and contractors that work, for any period of time, for or with the Trust.

4.1. Caldicott Guardian:

The Medical Director is the Caldicott Guardian. The Caldicott Guardian is accountable for the safe transfer of patient data. However each member of staff is responsible for patient confidentiality.

4.2. Senior Information Risk Owner (SIRO)

The SIRO is the Director of ICT, Estates and Facilities, and a mandated role which has overall responsibility for managing information risk across the Trust. They are also the owner of the Trusts Information Risk and Issues Register. The SIRO is a member of the Executive team and is assisted by;

- The Trust's Data Protection Officer- the Deputy Director of ICT – Information Services.
- The Trust's Deputy SIRO is the Director of ICT
- The Trust's Information Systems Security Officer is the Deputy Director of ICT – ICT Services
- The Information Governance Lead (ICT)
- An Information Asset Owner will be identified for each of the Trust's critical information assets.

4.3. Information Governance Lead

This role will lead the Information Governance agenda for the Trust and is accountable to the Deputy Director of ICT- Information. They will have day to day operational responsibility for all aspects of Information Governance (except information security and data quality).

4.4. Managers

It is the responsibility of all managers and supervisors of temporary staff, students and contractors who have access to sensitive personal information to ensure that staff are aware of the need for confidentiality under the Data Protection Act 1998. Managers and supervisors must make these individuals aware of the guidelines that need to be followed

in the handling of all sensitive personal information. Any staff not signed up to NHS Terms and Conditions must sign the Confidentiality Statement in Appendix 1.

4.5. All Staff

All members of staff are aware of the confidential nature of their employment and the sensitive information they may come across during their working day. All staff are provided with an introduction to Information Governance standards during their corporate induction and are expected to familiarise themselves with organisational policy in relation to these issues.

All staff are required to undertake mandatory information governance training on an annual basis.

A breach of confidentiality may result in disciplinary action in accordance with the disciplinary procedure and is seen as a serious offence which will be treated as gross misconduct and could result in dismissal. (See Disciplinary Policy).

5. MONITORING

Implementation of this policy will be monitored through carrying out regular audits across the Trust; interviewing staff and service users and regularly reviewing confidentiality incidents.

Incidents will be logged and reported to the Data Protection and Confidentiality Assurance Group, and where applicable taken to the Information Governance Steering Group (IGSG).

6. POLICY REVIEW

This policy should remain operational until superseded by an updated version. It is recommended to review this policy every two years, unless legislative or NHS guidance changes make it necessary to amend the policy.

7. DEVELOPMENT AND CONSULTATION

Consultation summary	
Date policy issued for consultation	
Number of versions produced for consultation	1
Committees / meetings where policy formally discussed	**Date(s)**
Data Protection & Confidentiality Assurance	16th July 2011
Information Governance Steering Group	23rd July 2011
Clinical Governance Committee	

Where received	Summary of feedback	Actions / Response
DP & Conf	Approved- guidance on external requests requested.	Guidance to be produced seperately
IGSG	Approved amendments	None required

8. REFERENCE DOCUMENTS

In writing this policy the author has made reference to the following documents.

1. Common Law of Confidentiality
2. Data Protection Act 1998 (DPA98)
3. Human Rights Act 1998 (HRA98):
4. Freedom of Information Act 2000
5. Access to Health Records Act 1991
6. Computer Misuse Act 1990
7. Administrative Law
8. Caldicott Report 1997
9. Confidentiality NHS Code of Practice 2003
10. Confidentiality: Protecting and Providing Information (GMC 2004)
11. Mental Capacity Act 2005

9. GLOSSARY/ DEFINITIONS

Commercially sensitive information

This is non-personal information (therefore not covered by the Data Protection Act), which may be sensitive to the Trust (e.g. some financial information) and therefore must be kept confidential.

Confidential Information

Information which can be classified as '**confidential**' is defined as information of a specific and personal nature about service users, their families or friends and carers, our employees and their families (e.g. health information, complaints, references etc) and other persons who are in contact with the Trust. In the context of Trust services, the simple fact of referral to a service would meet this definition and therefore all personal data held should be so classified.

'Confidential information' covered by this policy includes any information that has not been fully anonymised. If the name and address are not present but an NHS number is, then this is considered to be pseudo-anonymous, because it is still possible for the person to be identified (the NHS number is a unique identifier given to each person in England and Wales). Similarly, presence of date of birth and postcode may be sufficient, in combination with other information, to identify an individual. When producing statistical analyses it is important to not present data at too disaggregated a level as this may also lead to individuals being recognisable and others being able to infer confidential information.

Data

Data means information which –

1. is being processed by means of equipment operating automatically in response to instructions given for that purpose,
2. is recorded with the intention that it should be processed by means of such equipment,

3. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
4. does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
5. is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Emergency Situation

Situation which involve emergency services working with our staff (e.g. the evacuation of one of our inpatient facilities)

Explicit consent

The person was specifically asked and has given permission to record, store or disclose information. This would normally be supported by a written signed authorisation.

Implied consent

The individual has not been specifically asked for permission to record, store or disclose the information. The holder of the information assumes that permission was or would have been given by the individual concerned.

Care Record

A Service User's Care Record containing notes by all Health and Social Care workers involved in the treatment- can be paper and electronic. This may contain information not always written by BMSHFT staff (e.g. Birmingham Social Care staff and/or Solihull Care Trust staff who support BSMHFT teams).

Personal Information/Data

Data which relates to a living individual who can be identified from that data or from data and from other information which is in the possession of, or is likely to come into the possession of the data controller (e.g. our Trust) (Data Protection Act).

Sensitive Personal Information/ Data

The Data Protection Act 1998 also refers to 'sensitive personal data'. Special consideration and justification needs to be given for the collection and disclosure of such data. Sensitive personal data according to the Data Protection Act 1998 is:

- Physical or Mental Health or condition
- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade Union membership
- Sexual life
- The commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence any court in such proceedings.

From the above list it can be seen that most of the information the Trust collects and uses on service users (in clinical notes or electronically) and staff is considered to be '*sensitive personal information'* and subject to the highest level of protection under the Data Protection Act.

Treating Team

Any clinical staff within the Trust involved in the direct care and treatment of the service user.

Birmingham and Solihull NHS
Mental Health NHS Foundation Trust

APPENDIX 1: CONFIDENTIALITY AGREEMENT

I ……understand that whilst performing working for Birmingham and Solihull Mental Health Foundation Trust (BSMHFT) premises I may have access to confidential information, including personal information on service users and staff.

As such, I agree:

1. To take all possible steps to preserve strict confidentiality regarding any information to which I have access through my work. Including but limited to:
    a. Where information is stored.
    b. Not sharing login or password details.
    c. Reporting any incidents that occur.

2. Never to pass any information obtained to anyone outside the Trust, unless I have been directed to do so by a more senior member of staff within BSMHFT, and the reasons for doing so are clearly understood.

3. To keep all names, contact details and personal information secure.

4. To abide by the rules and guidance set out in the Trusts Confidentiality Policy and Care Records Policy.

I understand that any breach of the above will result in disciplinary action and/or may expose me to a suit for damages in a court of law.

By signing below I am confirming I will comply with the above, and am aware of the responsibilities placed upon me by the Trusts Confidentiality Policy (copy attached).

Signed: _____

Date: _____

Witnessed by (BSMHFT employee):

Print Name: _____

Signature: _____

Date: _____