Walsall Healthcare NHS
NHS Trust

Document Title
Confidentiality Policy

Document Description	
Document Type	Policy
Service Application	Trust Wide
Version	6.1

Lead Author(s)	
Name	Job Title
	Compliance and Risk Manager
	Corporate Governance Manager

Executive Director / Director / Manager			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date below:			
Name	Director of Strategy and Improvement	Date	May 2018
Signature			

Change History		
Version	Date	Comments
0.1	July 2011	New Policy
0.2	Feb 2012	Policy amendments following consultation
2.0	July 2012	Minor amendments following review
3.0	July 2013	Minor amendments following review
4.0	August 2013	Minor review following national changes to the Caldicott Principles
4.1	August 2014	Review following minor amendments
4.2	June 2015	Review following minor amendments
5.0	August 2016	Review following minor amendments
6.0	March 2018	Following review for General Data Protection Regulations
6.1	May 2018	Review following minor amendments

Links with External Standards	
General Data Protection Regulations	
Caldicott Principles	
Common Law Duty of Confidentiality	

Key Dates	DATE
Ratification Date	Trust Management Board – 26 June 2018 Minute Number 03/18
Review Date	June 2021

Executive Summary Sheet		
Document Title:	Confidentiality Policy	
Please Tick (□) as appropriate	This is a new document within the Trust	□
	This is a revised Document within the Trust	
What is the purpose of this document?		
The purpose of this policy is to outline the principles related to confidentiality and to support staff in applying these principles.		
What key Issues does this document explore?		
This policy identifies a person's (patients, staff or any other individual identified in trust records) expectations for confidentiality and specifies how Walsall Healthcare NHS Trust will undertake to protect those expectations. In addition this policy highlights how the Trust will comply with the laws on Data Protection, Human Rights, and Common Law Duty of Confidentiality etc.		
Who is this document aimed at?		
All staff working for Walsall Healthcare NHS Trust		
What other policies, guidance and directives should this document be read in conjunction with?		
GDPR Policy and Procedures Information Governance Policy Information Security Policy Information Risk Policy International Transfers of Personal Data Policy Mental Capacity Act Records Retention Policy Safe Haven Policy Patient Records Policy		
How and when will this document be reviewed?		
This policy will be reviewed in 1 year by the lead author or by a deputy nominated by the lead Director (or sooner if required).		

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
	Compliance and Risk Manager (Corporate Services)
	Corporate Governance Manager

Circulated to the following for consultation

Name/Committee/Group/	Designation
Intranet Forum	Wider consultation
Policies and Procedures Members	
Information Governance Steering Group	
MLCC Divisional Quality Board	
Surgery Divisional Quality Board	
Womens and Childrens Divisional Quality Board	

Version Control Summary

Significant or Substantive Changes from Previous Version
A new version number will be allocated for every review even if the review brought about no changes. This will ensure that the process of reviewing the document has been tracked. The comments on changes should summarise the main areas/reasons for change.

When a document is reviewed the changes should using the tracking tool in order to clearly show areas of change for the consultation process.

Change History		
Version	Date	Comments
0.1	July 2011	New Policy
0.2	Feb 2012	Policy amendments following consultation
2.0	July 2012	Minor amendments following review
3.0	July 2013	Minor amendments following review
4.0	August 2013	Minor review following national changes to the Caldicott Principles
4.1	August 2014	Review following minor amendments
4.2	June 2015	Review following minor amendments
5.0	August 2016	Review following minor amendments
6.0	March 2018	Following review for General Data Protection Regulations
6.1	May 2018	Review following minor amendments

1.0 INTRODUCTION

Respect for confidentiality is an essential requirement for the Trust.

The Caldicott Committee, which reported in 1997, was established to review the confidentiality and security requirements across the NHS with regard to personally identifiable information. The Committee recommended a series of six principles that should be applied when considering whether such confidential information should be shared.

All NHS organisations and Social Services Departments are now required to apply these principles and to nominate a senior person to act as a **Caldicott Guardian** responsible for safeguarding the confidentiality of person identifiable information.

Trusts are held accountable, through Clinical Governance, and now through Information Governance, for continuously improving confidentiality and security procedures. All Trusts are required to submit annual out-turn reports demonstrating progress made against their Caldicott improvement plans. This has recently been updated in light of the publication of the Information Governance Toolkit.

This policy links to Walsall Healthcare NHS Trust's policies covering Data Protection, Records Management and Information Management and Technology. These deal with the rights of people in respect of personal information held about them and the duties of the organisation to process personal information in a legitimate manner. The Records Management Strategy ensure information is held in a way which will ensure ready access and which will ensure information is disposed of, only at the appropriate times, and finally the Information Management and Technology Policy will ensure information is held in a secure environment. Together these policies form an integral part of the Trust's approach to Information Governance.

1.2 Scope and Limitations

The Trust and all staff who work for, or on its behalf, are subject to a Common Law Duty of Confidentiality. This duty of confidence only applies to personally identifiable information and not to aggregated or anonymised data.

1.3 Statement of Statutory Compliance

The guidance contained in the Caldicott Committee report is only one of a number of legal and statutory requirements; the Trust must comply with other guidance, related to maintaining the confidentiality, security and protection of person identifiable and anonymised information.

Key additional legislation and guidance includes, but is not limited to:

- Access to Health Records 1990
- General Data Protection Regulation
- Crime and Disorder Act 1998
- Human Rights Act 1998

- Freedom of Information Act 2000
- Health and Safety at Work Act 1974
- Children's Act 2004

2.0 POLICY AIM

The purpose of this policy is to outline the principles related to confidentiality and to support staff in applying these principles.

3.0 OBJECTIVES

Establish a Walsall Healthcare NHS Trust-wide approach to ensuring the confidentiality of personally identifiable information.

Inform members of the public, patients and carers about the Trust's confidentiality obligations and how it intends to meet them.

Inform staff working for, or on behalf of, Walsall Healthcare NHS Trust of their responsibilities with regards to confidentiality and personally identifiable information and how the Trust will enable these to be met.

4.0 DEFINITIONS

Confidentiality - when personal information is given or received in confidence for a particular purpose.

5.0 ROLES AND RESPONSIBILTIES

5.1 Chief Executive

Ultimate responsibility for data protection rests with the Chief Executive.

Medical Director (Caldicott Guardian)
Responsibility for ensuring that all patient related personal data is processed and managed in accordance with the Caldicott Principles. The Medical Director acts as the Trust's Caldicott Guardian with responsibility for patient confidentialty.

Director of Strategy and Improvement (Senior Information Risk Owner)
Responsibility for ensuring that all risks to information are identified and managed effectively in line with relevant legislation. The Director of Strategy and Improvement acts as the Trust's Senior Information Risk Owner (SIRO).

The Director of Strategy and Improvement has overall responsibility for the implementation, monitoring and compliance with the policy. This includes reporting to Trust executive groups or the Board as nescessary.

In addition, the Director of Strategy and Improvement has overall responsibility for:

- Information security
- Information governance
- Data quality related to patient information

Director of Organisational Development and Human Resources
Overall responisbility for ensuring data quality related to staff information and ensuring that the Trust standard contract includes clauses relating to staff responsibilities around information governance.

Corporate Governance Manager
Responsibility for ensuring there are information governance arrangements in place to allow for the processes laid out within this policy and procedure.

Data Protection Officer
Walsall Healthcare NHS Trust have appointed a Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with others to ensure that all processes, systems and staff are operating compliantly and within the requirements of the GDPR and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the GDPR and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

The Data Protection Officer has assumed the below duties in compliance with GDPR Article 39: -

- To inform and advise Walsall Healthcare NHS Trust and any employees carrying out processing, of their obligations pursuant to the GDPR, the Supervisory Authorities guidelines and any associated data protection provisions

- To monitor compliance with the GDPR, associated data protection provisions and Walsall Healthcare NHS Trusts own data protection policies, procedures and objectives

- To oversee the assignment of responsibilities, awareness-raising and training of

staff involved in processing operations

- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs

- To cooperate with the Supervisory Authority where required

- To act as the point of contact for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter

- In accordance with Article 35 (type of processing is likely to result in a high risk to the rights and freedoms of natural persons), the DPO will provide advice where requested with regards to any data protection impact assessment and monitor its performance pursuant

- Have due regard to, and be aware of, the risk associated with processing operations, considering the nature, scope, context and purposes of processing

Designated Data Protection Officer
NAME: Sharon Thomas
POSITION: Corporate Governance Manager
ADDRESS: Walsall Healthcare NHS Trust, Town Wharf, Block 3, Cavell Close, Walsall
EMAIL:sharon.thomas@walsallhealthcare.nhs.uk or data.protection@walsallhealthcare.nhs.uk
TEL: 01922 721172 ext 5806

Health Records Manager
Overall responisbility for ensuring the appropriate records retention and destruction standards are adhered to.

Information Asset Owners
Any member of staff who has assigned responsibility for an information asset within the Trust (i.e. any system (electronic or paper based) that holds Trust information) is designated an Information Asset Owner for the purposes of information governance.

Privacy Officers
It is the responsibility of the Trust's Privacy Officer's to investigate any breaches of confidentiality regarding information accessed via the Spine.

Information Governance Steering Group
The Information Governance Steering Group (IGSG) will have overall responsibility for:

- The updating and amending of this, and all over information governance policies
- Monitoring the action plans for the Information Governance Toolkit (IGT) and the information governance work plan
- Ensuring the statutory regulations around information governance are adhered to

Data Quality Team
The Data Quality Team are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified.

IT Department
The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed.

Only the IT Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally.

Divisional Directors (DD; or equivalent)
Managers are considered to be equivalent to DD's for the purpose of responsibilities under policies if they are responsible for management of a significant service and report directly to an Executive or Associate Director.

Responsibilities include implementation, monitoring and compliance within the Division and ensuring staff witih the division adhere to the requirements of the policy.

Matrons, Senior Sisters (with day to day responsibility for ward management), Departmental Managers or equivalent
This group will be responsible for day to day implementation of the policy.

Also included will be responsibility for ensuring:

- All staff are aware of their role under the policy
- Staff complete their mandatory annual information governance training
- Records are kept as specified
- Incidents / issues are reported

All Staff
All staff must ensure they understand and adhere to the requirements of this policy.

6.0 PROCEDURE

6.1 Context

Walsall Healthcare NHS Trust provides health services to a population of some 260,000 residents of Walsall as well as referrals from surrounding Health Areas. In providing these services, it is necessary that staff communicate personal information about patients to other organisations. These include GP Practices, Walsall CCG, dentists, pharmacies, opticians, social services and other voluntary groups.

In all instances the confidentiality of patient information must be considered and care taken to ensure that the rights of the patient under the various legislation is not breached.

In addition, Walsall Healthcare NHS Trust employs some 3000+ staff, each of which has employee records which are due the same level of confidentiality as patient records. The extension of this confidentiality policy to include staff records is covered by Appendix IV**.**

Irrespective of where, how, with or to whom else Walsall Healthcare NHS Trust provides its services, the requirements for confidentiality remain of the same high standard and apply to all individuals who have worked or are working for, or on behalf of, Walsall Healthcare NHS Trust.

Following a widespread public consultation in 2002, the Department of Health has developed a nation-wide confidentiality code of practice for all NHS staff. The content of this policy takes into account the content of that Code of Practice.

In the course of their duties, any member of staff may have access to confidential material about patients, members of staff or other health service business. Information relating to identifiable patients must not be divulged to anyone other than an authorised person, for example medical, nursing or other professional staff, as appropriate, who are concerned directly with the care, diagnosis and/or treatment of the patient. Senior staff, eg the Caldicott Guardian, will be consulted if there is any doubt as to the authority of a person to request personal information about a patient. The Trust considers any breach of confidentiality in a serious manner and will take disciplinary action against anyone found to have broken confidences. Dismissal may result. Confidentiality clauses covering these issues appear in all contracts of employment.

6.2 Patient Experience

The patient/client has a right to believe that information given to a health care professional is given in confidence in the expectation:

- That it will be used only for the purposes outlined in the patient publications and will not be released to others without their consent.

- That it will be held in private and secure storage.

- That, where it is deemed appropriate to share information obtained in the course of professional practice with other health or social work practitioners, or in the case of children, education services, the health care professional who obtained the information must ensure, as far as is reasonable, before its release that it is being imparted in strict professional confidence and for a specific purpose.

- That where it is deemed appropriate to share information obtained in the course of professional practice with other health and social work practitioners, or in the case of children, education services, the patient client is aware of this, the reasons for it and where there may be disclosure of information to others not directly involved in the client's/patient's care given the opportunity to withhold

consent.

- That the responsibility to disclose or withhold confidential information lies with the individual practitioner.

- That he/she cannot delegate the decision.

- That he/she cannot be required by a superior to disclose or withhold information against his/her will.

- That a health care professional who chooses to breach the basic principle of confidentiality in the belief that it is necessary in the public interest including that of protecting a child must have considered the matter sufficiently to justify that decision.

- That deliberate breaches of confidentiality other than with the consent of the patient/client will be exceptional.

- That when a health care professional is considering disclosure of confidential information, Walsall Healthcare NHS Trust has a duty to ensure that the individual staff member can seek and gain appropriate advice through their line manager, their professional body and Caldicott Guardian who may wish to consult the Trust's legal advisors.

6.3 Principles of Confidentiality

6.3.1 *General Principles*

Confidential information may not then be used for a different purpose or passed on to anyone else without the consent of the information provider.

However, there may be occasions when it could be detrimental to the patient or to another individual if this principle is strictly adhered to.

An example of such an exception would be child protection where the overriding principle is to secure the best interests of the child. Anyone holding information that is relevant to the protection of a child/children **must** share that information with others on a strictly controlled basis. Several major child abuse inquiries have identified the lack of such communication as being a contributing factor in the death of a child.

Most breaches of confidence are unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security. However, the consequences could be equally serious for all concerned. The simple rule of thumb is that personally identifiable information will always be held securely and, when used, treated with respect. This rule applies whether the information is held manually or in a computer, on video or audio tape or in a member of staff's head.

6.3.2 *Caldicott Principles*

The following seven Caldicott principles will be adhered to in all cases where the appropriate use of person identifiable health information is considered.

Principle 1 Justify the purpose(s) - every proposed use or transfer of personal confidential data within or from, an organisation should be clearly defined, scrutinized and documented, with continuing uses regularly reviewed by an appropriate guardian

Principle 2 Don't use personal confidential data unless it is absolutely necessary – personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 Use the minimum necessary personal confidential data - where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out

Principle 4 Access to personal confidential data should be on a strict need to know basis - only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes

Principle 5 Everyone with access to personal confidential data should be aware of their responsibilities - action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 Comply with the law - every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements

Principle 7 The duty to share information can be as important as the duty to protect patient confidentiality – health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by policies of their employers, regulators and professional bodies.

Examples of justifiable purposes include:

- Delivering personal care and treatment
- Assuring and improving the quality of care and treatment
- Monitoring and protecting public health
- Managing and planning services
- Contracting for the NHS
- Auditing NHS accounts and accounting for NHS performance

- Risk management
- Investigating complaints and notified or potential legal claims
- Teaching
- Statistical analysis
- Medical or health services research

Appendix II provides guidelines for staff on key factors relating to confidentiality.

These guidelines do not and cannot provide definitive answers for every situation as much depends on the context of the individual case. If in doubt staff will seek appropriate advice before releasing personally identifiable information.

6.4 Meeting the requirements for confidentiality

People have a right to expect that information about them, provided or discovered in the course of their health care, will be held in confidence. Without assurances about confidentiality, people may be reluctant to provide information and this could lead to unnecessary restrictions on what most people rightly perceive as the essential purpose of providing it: the delivery of appropriate and effective care to themselves.

To meet confidentiality requirements of patients, carers and staff, Walsall Healthcare NHS Trust has, or has in development, the following policies, procedures and/or processes in place:

- Confidentiality and Data protection staff training and induction programme
- GDPR Policy and Procedures
- Access to Health Records procedures
- Records Retention Policy
- Information Management and Technology Policy
- Information Sharing Protocol
- Safe Haven Policy
- Data Breach Policy
- Information Governance Toolkit

All staff throughout the Trust have a responsibility for maintaining confidentiality and will be aware of how the content of the above-mentioned policies, procedure and processes affects their actions on a day to day basis.

6.5 Guidelines for the Protection of Confidentiality

6.5.1 *Guidelines for the Protection of Confidentiality*

(If in doubt – check it out - before releasing personally identifiable information)

Decision trees in Appendix III identify the processes for disclosing information under three different circumstances, i.e. where it is necessary in order to provide healthcare, where it isn't to provide healthcare but it is a medical purpose as defined in legislation and where the purpose is unrelated to healthcare or another medical purpose. These

have been defined in the “NHS Code of Practice: Confidentiality”.

6.5.2 *Obtaining Consent*

As a general rule personal information given for one purpose may not be disclosed to a third party or used for another purpose without the consent of the person it relates to, unless the third party is at risk.

Within the Health Service it may not be practical to obtain the consent of the patient every time information needs to be shared with other professionals involved in the care of that patient. Therefore it is necessary for the Trust to remind patients of their rights regarding confidentiality and inform them in what circumstances and for what purposes their personal information may be shared.

All new patients will be provided with Walsall Healthcare NHS Trust’s leaflet which explains why personal information about them may need to be shared with other professions and agencies. Similarly, at a patient’s first appointment, clinicians will take the opportunity to discuss and explain the need for the sharing of personal information. Specific consent to the sharing of person identifiable information must always be sought for situations not covered by the Trust’s leaflet and in particular when information has to be shared with services outside the Walsall Healthcare NHS Trust. In these cases the clinician will provide the patient with a verbal description as to how the information will be used and then make a dated comment in the case notes as to the patient’s decision

In this latter case, the patient will be advised that, if consent is withheld, there could be implications for the quality of care that can be offered. The clinician will, with the patient, investigate the reasons for withholding consent and attempt to arrive at a satisfactory solution where the care given would be least compromised.

6.5.3 *Informing Relatives*

Whilst the routine provision of information about a patient’s condition to a near relative or a person with a close relationship to the patient should not be obstructed unnecessarily, the provision of information will be at the discretion of the service and will reflect any wishes of the patient.

If before death a patient gives requests that the relatives or carers do not see their medical records, then this must be recorded in the Patient Record and the wish respected after death.

Under Caldicott, the clinician has the ultimate decision regarding the sharing of the medical notes with other parties, providing it is done with the express purpose of helping the patient. It is a responsibility which cannot be delegated. Advice can be sought from other clinicians (typically the Caldicott Guardian) or from the relatives and carers, but ultimately the decision lies with them.

The relatives or carers have no over-riding power to give consent on behalf of the patient, unless acting with power of attorney.

If the patient is under 18, information may be passed to their guardian unless they

expressly oppose this or unless the professional involved felt that this would put the child at risk.

If the child has a life threatening condition the parents or guardian will be approached regardless.

6.5.4 *Withholding Information*

If a patient requests that a specific piece of personal information be withheld from someone then this view should be respected, unless there are overriding considerations. The reason the patient gives for not passing on the information must be noted. An overriding consideration may include the statutory obligation that staff have to work together with other agencies as stated in the Children's Act 1989 and the Mental Health Act 1983.

6.5.5 *Consent of Children*

Children under the age of 18 who in the view of the health care professional have the capacity and understanding to take decisions about their own treatment, are entitled to decide whether personal information may be passed on. This may be particularly relevant if a child does not wish his/her parent to know. However, the child will be encouraged to involve parents or other legal guardians.

If the child has a life threatening condition the parents or guardian will be approached regardless.

Relevant dated comments will be placed in the patient records identifying decisions and judgments made.

6.5.6 *Inability to Give Consent*

If for any reason a patient is incapable of giving consent for their information to be shared, the professionals concerned (who may or may not be part of a multi disciplinary team) would make the decision, taking into account the best interest of the patient in line with the principles of the Mental Capacity Act. This will include considering the views of relatives, carers or advocates, and any views the patient may have had, if at some stage he/she had the capacity to decide.

However, the clinician cannot delegate that responsibility to share or not share that information. Providing adequate consultation has taken place with line managers and the Caldicott Guardian, then Walsall Healthcare NHS Trust is obliged to support that clinician's decision, even if they choose to go against the advice given.

Relevant dated comments will be placed in the patient records identifying decisions and judgments made.

6.5.7 *Retention and Disposal of Information*

The retention and disposal of personal information in either a manual or computer format is addressed in the "Records Management Strategy and Policy" and the "Disposal of

Media Policy". Information from which a person can be identified must always be disposed of securely.

6.5.8 *Disposing of Electronic Data*

For guidance on the disposal of electronically stored data that includes personal information, the Trust's Information Technology Department, or the Officer with delegated Caldicott responsibility will be contacted.

6.5.9 *Recording of Information*

Decisions regarding the use of personal information will be clearly recorded within the individual patient's records and authorised by the member of staff responsible for making the decision.

6.5.10 *Confining Information*

Within the Trust a large number of staff, both professional and administrative will see personal information. It is therefore vital that the principle of confidentiality is maintained. This would include all personal information about members of the public, not just their medical records. Names will not be exchanged unless there is a need to do so.

6.5.11 *Sharing Information*

The seven Caldicott Principles will be adhered to in all cases where the sharing of personally identifiable information is being considered. In addition, if information is being shared outside the NHS, a formal Information Sharing Protocol will be implemented.

6.6 Occasion for Disclosure

Disclosure of confidential information should only occur if the individual gives consent *or* on a "need to know" basis if the reasons are deemed justifiable. Section 7 of the Health and Safety at Work Act states that if a risk is identified to someone else's health and safety and that person is not informed of the risk, the individual identifying the risk is in breach of the Act. This may include information regarding a patient or carer, which may put others at risk.

6.6.1 *Seeking Advice*

In the event that the Health Care Professional responsible for the patient's care is required to pass on information, they are responsible for passing the *minimum* information necessary for the purpose. If needed, they should take advice from a senior professional or manager who may themselves seek advice from the Caldicott Guardian or the Health Records Manager.

6.6.2 *Breaking Confidentiality*

If a health care professional chooses to break confidentiality because it is deemed to be in the best interest of the public, e.g. due to the violent history of a patient, the decision must be carefully considered as it may need to be justified. In such a case, the health

care professional will consult their manager, who will then seek advice from the Caldicott Guardian. Such decisions will be clearly recorded in the patient's records.

6.6.3 *Protecting the Public*

There may be instances when staff working for, or on behalf of the Trust feel obliged to pass on information to protect the public or for the purpose of averting a serious crime. This type of disclosure will be made in consultation with the Medical Director who also has responsibility for Clinical Risk, unless specifically allowed within one of the Trust policies. When decisions of this type are taken, a permanent record of the decision will be made and held in an appropriate place. Each case will be considered individually but it may be necessary to seek advice from a manager. Further advice may be sought from the Trust's Caldicott Guardian and, on occasions, legal advice through the director responsible for Clinical Risk. There is no absolute definition of "serious crime", but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences". These include:

- treason
- murder and manslaughter
- rape and certain sexual offences
- kidnapping and the taking of hostages
- causing an explosion and offences under the prevention of terrorism legislation
- certain firearm offences
- hijacking
- causing death by reckless driving
- making a threat which if carried out would be likely to lead to:
  - i. a serious threat to the security of the state or to public order.
  - ii. serious interference with the administration of justice or with the investigation of an offence
  - iii. death or serious injury
  - **iv.** substantial financial gain or serious financial loss to any person

6.7 Information to the Media

As a general rule no information is to be given to the media in respect of current or previous patients, carers or staff. The passing of personal information to the press or media is covered by the same general principle, that is, if the person whom the information is about is capable of taking a decision their consent must be obtained. Likewise if the individual is incapable of making the decision, information should only be given if it is in the best interests of the person concerned. The Director of Strategy, who has responsibilities for communications will decide who is the most appropriate member of staff to speak to the media. The issue of providing information to the media is covered in the "Procedure for Dealing with Media Enquiries"

6.8 Multi-agency Protocols

Where at all possible, multi-agency protocols will be developed to cover the transfer of information. The officer with delegated Caldicott responsibility can give advice.

6.9 Ensuring Confidentiality

- Clear desk / clear screen policy
- VDU Positioning so no-one else can see the screen
- Ensuring conversations are not overheard
- Ensuring information is received by the right people
- Fax Machines located in Safe Havens (Safe Haven Policy)
- Secure emails (Safe Haven and Information Management and Technology Policy)

6.10 Processing Information Requests

When information is requested from anyone other than the subject, a clinician, someone acting on behalf of a clinician (i.e. a medical secretary), or some other authorised person (ie audit, clinical governance, complaints, etc) the provision of identifiable information will be avoided. The possible methods of providing unidentifiable information are as follows

- **Anonymisation** - Information should be non-identifiable. Under data protection even a code number (i.e. NHS Number) which can be related back to an individual, no matter how closely guarded that code is, makes the information identifiable. Small samples with postcodes will similarly make identification possible.

- **Aggregated Data** - Again small sizes of samples could lead to identification and therefore should be avoided. If there is no alternative to using small sample sizes then the patient will be made aware that aggregated and statistical info will be prepared using their data. They will however be advised that there could be a risk of them being identified due to that small sample size. If they agree then it is all right to continue. Should they refuse consent then their data should not be used in the sample.

6.11 Teaching and Research

Advice to patients about the use of personal information must emphasize:

- the importance of teaching and research to the maintenance and improvement of care within the NHS

- that such information, anonymised or aggregated wherever possible, may sometimes be used for teaching and research (and that universities or other bodies carrying out approved research are required to treat it in confidence and must not use it for other purposes)

- that any research proposals involving access to patient records require clearance by the relevant Local Research Ethics Committee. (LREC approval is not required for epidemiological surveys conducted for the purpose of communicable diseases surveillance and control)

- the Local Research Ethics Committee must be satisfied in particular that:
  i. arrangements for confidentiality are satisfactory.
  ii. any additional conditions relating to the use of information that the LREC thinks are necessary can be met.
  iii. any application to use identifiable patient information is fully justified e.g. because this is essential to a study of major importance to public health. If not, approval would not be given.

- that their specific consent will be sought to any activity relating to teaching or research that would involve them personally

- that published research findings will not identify them without their specific agreement.

6.12 Restrictions on passing on information

NHS bodies or those carrying out NHS functions must not allow personal details of to be passed on or sold for fund-raising or commercial marketing purposes.

There are some statutory restrictions on the disclosure of information relating to HIV and AIDS and other sexually transmitted diseases, assisted conception and abortion.

Under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000, every NHS Trust and Primary Care Trust shall take all necessary steps to secure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except-

(a) for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof, and

(b) for the purpose of such treatment or prevention.

6.13 Confidentiality of staff and other personal information

General Data Protection Regulation, the Common Law Duty of Confidentiality, and the Human Rights Act 1998 all apply equally to personal information of any description, not just Health Records. Appendix iv contains additional guidance on dealing with this type of information.

7.0 IMPACT ASSESSMENT

7.1 Financial implications

The GDPR imposes substantial fines on data controllers and processors for non-compliance.

Fines are administered by the individual member states supervisory authorities; i.e. The Information Commissioner. These fines are categorised in two levels; lower level which may result in a fine of up to £7.9M, or 2% of the worldwide annual revenue of the prior financial year, whichever is greater or upper level which could be up to £17.5M, or 4% of the worldwide annual revenue, whichever is greater.

The upper level fine could be issued for infringements of the basic principles for processing, including conditions for consent, the data subjects' rights to access and the transfer of personal data to a recipient in a third country or an international organisation.

7.2 Risk Implications / Risk Assessment

None

7.3 Discrimination or other adverse effects on population groups

The impact of this policy has been assessed. It will not lead to any discrimination or other adverse events on population groups in relation to:

Ethnicity / Gender / Age / Sexuality / Religion or Belief / Disability / Status as Transgender or Transsexual Person.

8.0 MONITORING, CONTROL AND AUDIT

Monitoring Process	Requirements
Who	Officer with Caldicott Authority
Standards Monitored	Breaches of confidentiality
When	Annual
How	Audit of breaches of confidentiality using confidentiality audit procedures
Presented to	Information Governance Steering Group
Monitored by	Information Governance Steering Group
Completion/Exception reported to	Quality and Safety Committee

9.0 BEST PRACTICE, EVIDENCE AND REFERENCES

Access to Health Records Act 1998
General Data Protection Regulation
Crime and Disorder Act 1998
Human rights act 1998
Freedom of Information Act 2000
Criminal Procedures and Investigations Act 1996
Regulation of INVESTIGATORY Powers Act 2000
Health and Social care Act 2001
NHS (Venereal disease) Regulations 1974
Human Fertilisation and Embryology Act 1990
Abortion Regulations 1991

Appendix 1

Confidentiality Audit Procedure

1. Procedure(s)

1.1 Monitoring Access to Confidential Information

In order to provide assurance that access to confidential information is gained only by those authorised to do so, appropriate monitoring must take place on a regular basis.

Monitoring should be carried out by the appropriate Informaiton Assest Owner (IAO) in order to identify any irregularities around access. These irregularities should then be reported to either the Trusts Data Protection Officer or the Caldicott Guardian (CG) and action taken to address the issues.

Actual or potential breaches of confidentiality must be reported to the Trusts DP Lead and CG, via the Caldicott email, immediately to ensure that action can be taken to prevent further breaches. Incidents should also be reported via the online reporting tool accesible on the home page of the intranet.

Should unauthorised access to confidential information be gained by any individual, this will be dealt with in accordance with the Trust's disciplinary procedures.

1.2 Auditing Access to Confidential Information

The CG (or nominated deputy i.e. DP Lead) will ensure that audits of security and access arrangements within each area are conducted on a annual basis.

Areas to be audited should include:

- Security applied to paper based documentation
- Arrangements for recording access to paper based documentation (e.g. subject access requests, tracking logs etc.)
- Evidence that checks have been carried out to ensure that the person requested access has a legitimate right to do so
- The existence and location of whiteboards containing personal information
- The use of, and disposal arrangements for, post-it notes, notebooks and other temporary recording materials
- Retention and disposal arrangements
- The location of fax machines and answerphones which may receive confidential information – are they designated safe havens?
- Security arrangements applied to any documentation that is removed from the workplace
- The understanding of staff within the department of their responsibilities with regards to confidentiality and restrictions on access to confidential information
- Security applied to laptops and compliance with the Trusts IM&T policy
- Evidence of shared passwords being used within the area being audited

1.3 Audit Method

The audit should be carried out through informal interviews with members of staff within the department being audited (across all levels). Interviews can take place on a one to one basis or as groups.

As a last resort questionnaires can be used in place of interviews, however this will not gather the quality of results that interviews will.

1.4 Frequency

Prior to commencing the audit process, it will be necessary to decide how frequently audits will be carried out. It is recommended that each area is audited once per year. A programme of audits should be produced detailing the date on which each area will be audited. Each audit should have a unique reference number which can be used on all documentation relating to the audit.

Once the audit programme has been produced, this should be submitted to the Information Governance Steering Group (IGSG) for approval prior to implementation. Once approval is gained the programme should be communicated to all Heads of Service / Managers / Heads of Department / Team Leaders affected to ensure that they are aware when their audit will take place.

1.5 Choosing Appropriate Auditors

Audits should be conducted by individuals who have no connection with the work function being audited to ensure that the audit is undertaking objectively.

It is recommended that auditors undertake appropriate training prior to commencing the audit process, however this is not mandatory.

Auditors should have a good working knowledge of the requirements of the General Data Protection Regulations, Caldicott Principles, Records Management Processes and an overview knowledge of general Information Governance principles.

Individuals conducting audits should:

- Demonstrate an objective and responsible approach
- Possess sound judgement, excellent analytical skills and tenacity
- Demonstrate a rational approach to diverse situations
- Demonstrate an ability to understand complex processes
- Demonstrate the ability to understand the role of the role being audited in relation to the Trust as a whole

1.6 Pre Audit Questionnaires

To assist in the audit process completion of a pre audit questionnaire will enable the auditor to gain an understanding of the function of the area to be audited and

the processes carried out relating to confidential information.

The pre audit questionnaire should include the name of the department / area, a contact name and number and should be returned to the auditor by the date stated.

1.7 Pre Audit Meeting

The auditor should arrange a brief pre audit meeting with the Head of the area / department to be audited with the aim of discussing who will be involved in the audit; how long the audit is likely to last; what documentation will be required; what facilities will be required (e.g. workspace) and what feedback will be provided to the Departmental Head. The required documentation should be forwarded to the auditor prior to the audit commencing, this should include any local procedures that are in place.

1.8 Audit Checklist

An audit checklist (see appendix C) should be produced which will enable the auditor to track the progress of the audit

1.8.1 Conducting the Audit

Questioning Techniques

Initially ask the question to establish the fact, listen to the response then confirm you have understood correctly. Confirm that the information you have been given corresponds with the documented procedures, then check records and logs to ensure that they demonstrate that the procedures have been followed. Also check that any records and logs are up to date.

Brief notes should be made on the Audit Checklist.

Column B should be used to record evidence put forward to support responses to questions.

Column C should be used to record the auditors assessment of the evidence provided and how it demonstrates compliance with the requirements of the Data Protection Regulation Trust policies and procedures and the Caldicott Principles.

Column D should be used to record the auditors grading of the response to each question. The following codes should be used when grading responses:

- COM – evidence demonstrates full compliance
- MAJ – evidence demonstrates major non compliance
- MIN – evidence demonstrates minor non compliance
- OBS – no evidence of non compliance was found, but an observation was made that there was the potential for problems to occur and improvements which could be made

1.8.2 **Staff Awareness Interviews**

Staff awareness interviews give an opportunity for the auditor to assess the level of awareness of confidentiality issues.

Interviews can be conducted on either a one to one or group basis for between 15 and 30 minutes.

The interview should be conducted using directed questioning techniques, starting with broad questions relating to a particular topic, following up with further questions to gradually narrow the scope of the question.

Pre-set questions should be used to establish:

- Roles and responsibilities
- Awareness of general confidentiality issues
- Understanding of the Data Protection Principles directly relating to their job role
- Understanding of the requirements of policies, protocols and procedures relating to confidentiality
- Training received

The auditors questions and interviewee(s) response should be recorded on the Interview Record Sheet (see Appendix E)

During the interview process the auditor should ensure that all observations are recorded (rather than only negative observations) to ensure a balanced result to the audit.

1.8.3 **Reporting**

A formal report should be provided to the area audited detailing the audits outcomes. Audit reports and any associated action plans should also be reported to the IGSG by either the DP Lead or the CG.

1.8.3.1 **Non Compliance**

Where non compliance is observed this should be recorded as soon as possible, in sufficient detail, including all the relevant facts and evidence. Non compliance should be recorded on the Non Compliance Observation sheet (Appendix D). The detail recorded should include what was observed; where it was observed; who was involved; the date of the observation and why it was considered non compliant.

Each non compliance should have an associated action / recommendation which should be discussed with the Departmental Head / Manager. Recommendations should also have a target date for acheivement and a named individual responsible for the recommendation completion.

Once the feedback meeting has taken place the auditor will complete the bottom section of the inform to indicate the implementation and effectiveness of the

recommendations. When the auditor is satisified that the non compliance has been resolved the auditor will sign the Non Compliance Observation Sheet.
Non Compliance can be either:

- Major – indicating that the non compliance has occurred on a regular basis and could have potentially serious consequences
- Minor – indicating either a one off occurrence and that there is little risk of non compliance having any more than a minor consequence

1.8.3.2 **Concerns Observed**

There may be incidences where the auditor is concerned by what has been observed, but the incidences are not actual non compliances. In this case the auditor can make recommendations for improvements to be made to the departments practice in order to ensure that potential problems do not occur. A Recommendations Sheet should be completed (see Appendix F)

1.8.4 **Audit Report**

The report should be produced once the audit has been completed. The report should include a summary of the findings of the audit, together with any observations of non compliance, recommendations made, the date of any follow up meetings should also be included. The Trust standard report template should be used for the audit report.

1.8.5 **Closing Meeting**

This meeting allows the auditor to present the findings from the audit. The audit summary, detailed findings, recommendations for improvement and timescales for improvements should be discussed.

Agreement should be gained from the Department Head / Manager re: any non compliance issues observed. Any comments expressing disagreement should be noted on the audit documentation.

1.8.6 **Audit Follow Up**

Once the audit process is complete arrangements should be made for a follow up meeting where non compliance has been observed. This will allow the auditor to confirm that the recommendations have been actioned. Should any non compliance be related to documentation the revised documentation should be reviewed to ensure the actions have been completed.

1.8.7 **Audit Closure**

Once the auditor has confirmed that all recommendations have been actioned the audit can be formally closed.

Confidentiality Audit Programme

Department / Area	Audit Frequency	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar
e.g. Imaging	*Annual*												

Confidentiality Audit
Pre-Audit Questionnaire

Department / Area:		**Audit Reference:**
Division / Directorate:		
Contact Name:	**Job Title:**	**Ext:**
Summary of Department / Area Functions:		
F/T Staff:	**P/T Staff:**	

Audit Questions:

Question 1	*Enter question here*
Question 2	*Enter question here*
Question 3	*Enter question here*
Question 4	*Enter question here*
Question 5	*Enter question here*
Question 6	*Enter question here*

Confidentiality Audit
Audit Checklist

Department:		**Interviewee:**		**Page No:**
Process:		**Auditor:**	**Audit Ref:**	**Date:**
Question (A)	**Evidence (B)**	**Findings & Observations (C)**		**Result (D)**

Confidentiality Audit
Non Compliance Sheet

<table>
<tr><td colspan="2">Department / Area:</td><td>Audit Date:</td><td>Audit Ref:

Observation Ref:</td></tr>
<tr><td colspan="4">Details of Non Compliance:</td></tr>
<tr><td colspan="2">Extent of Non Compliance: (tick as appropriate)</td><td>Auditor Name:</td><td rowspan="2">Date of Observation:</td></tr>
<tr><td>Major</td><td>Minor</td><td>Signature:</td></tr>
<tr><td colspan="4">Recommendations:</td></tr>
<tr><td colspan="2">Follow Up Date:</td><td colspan="2">Additional Comments:</td></tr>
<tr><td colspan="4">Follow Up Notes:</td></tr>
<tr><td colspan="2">Compliance Assessment (delete as appropriate):</td><td>Auditor Name:</td><td rowspan="2">Date Re-assessed:</td></tr>
<tr><td colspan="2">COM / MAJ / MIN</td><td>Signature:</td></tr>
</table>

Confidentiality Audit
Interview Record Sheet

Department / Area:	**Audit Date:**	**Audit Ref:**
		Page No:

Attendees:	
Name:	**Job Title:**

Question 1	*Enter question here*
Question 2	*Enter question here*
Question 3	*Enter question here*
Question 4	*Enter question here*
Question 5	*Enter question here*
Question 6	*Enter question here*

Confidentiality Audit
Recommendations Sheet

Department / Area:	**Audit Date:**	**Audit Ref:** **Page No:**
Details Observed:		
Auditor Name:	**Signature:**	**Date of Observation:**
Recommendations:		
Follow Up Date:	**Additional Comments:**	
Follow Up:		
Auditor Name:	**Signature:**	**Date Re-Assessed**

APPENDIX 2

LEGISLATION SURROUNDING CONFIDENTIALITY

1.1.1 *Access to Health Records Act 1990*

This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

1.1.2 *General Data Protection Regulation*

Data Protection legislation governs the standards for the processing of personal data including the collection, use of and disclosure of such information. The legislation requires that data controllers meet certain obligations. It also give individuals or 'data subjects' certain rights with regard to their own personal data.

The main standard for processing personal data as set out in article 5 is compliance with the six data protection principles summarised as follows:

i) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
ii) Personal data shall be collected for specified, explicit and legitimate purposes
iii) Personal data shall be adequate and limited to what is necessary

iv) Personal data shall be accurate and up to date

v) Personal data will be held for no longer than is necessary.

vi) Personal Data will be processed in a manner that ensures appropriate security

1.1.3 *Crime and Disorder Act 1998*

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information and responsibility for the disclosure remains with the agency that holds the data.

The Criminal Procedures and Investigations Act 1996 requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

1.1.4 *Human Rights Act 1998*

Article 8.1 of the Human Rights Act 1998 provides that "everyone has the right to respect for his private and family life, his home and his correspondence". This is, however, a qualified right i.e. there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides "there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others".

In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show in relation to its decision to take a particular course of action:

- that it has taken these rights into account
- that it considered whether any breach may result, directly or indirectly, from the action, or lack of action
- if there were the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights
- whether one of the permitted grounds for interference could be relied upon
- whether there was proportionality

The Act also requires public bodies to read and give effect to other legislation in a way which is compatible with these rights and makes it unlawful to act incompatibly with them. As a result these rights still need to be considered, even when there are special statutory powers to share information.

1.1.5 *Common Law Duty of Confidentiality*

All staff working in both the statutory and independent sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specified individual.

The Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm). Whilst it is not entirely clear under law whether or not a common law Duty of Confidence extends to the deceased, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained (deceased individuals may have provided their consent prior to death). Articles 6 and 9 of the General Data Protection Regulations apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness) other conditions in Articles 6 and 9 of the General Data Protection Regulations must be satisfied (processing will normally need to be in the vital interest of the individual).

Whilst under current law no-one can provide consent on behalf of an adult in order to satisfy the common law requirement, it is generally accepted that decisions about treatment and the disclosure of information should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

All agencies are subject to their own codes or standards relating to confidentiality**.**

1.1.6 *Freedom of Information Act 2000*

This Act provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector. The release of personal information remains protected by the General Data Protection Regulation.

1.1.7 *Other legislation – summary details not provided*

Criminal Procedures and Investigations Act 1996
Regulation of Investigatory Powers Act 2000
Health and Social Care Act 2001 (Section 60)

1.1.8 *There are statutory restrictions on passing on information linked to:*

- NHS (Venereal Disease) Regulations 1974
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991

1.1.9 *Third Party Disclosures*

This applies when information is shared between organisations/agencies for a defined purpose then passed onto either another agency without consent or used for a different purpose without securing the consent from the original provider.

Controls surrounding this should be made clear in the specific Information Sharing Protocol addressing how information should be shared between the agreed parties.

APPENDIX 3

CONFIDENTIALITY CODE OF CONDUCT FOR STAFF

WALSALL HEALTHCARE NHS TRUST

STAFF CODE OF PRACTICE: - CONFIDENTIALITY

Do not breach confidentiality (personal and/or patient)- Safeguard confidential information by following the basic rules listed below.

Do not disclose personal information to anyone who is not authorised to receive it. This includes Trust and other NHS and social care staff not directly involved in the care of the patient/person.

Keep your computer or security passwords secure and do not let any other person have them. If you suspect someone knows your password then you will immediately change it, seeking help if necessary. Contact your manager and advise them of a potential breach of security and then complete an "Untoward Incident Form" and submit it to the Risk Management Department. Do not write down your password.

Do not use someone else's password to gain access to information. All systems have the facility to 'audit' who accesses them, at what time and on what date. If you don't have a password for a system, then you are not authorised to use that system. It will be a breach of discipline if you continue to try to access that system. If for work purposes you need that access then arrange to be trained on the relevant system and get your own password.

Log out of the computer system when leaving it unattended. This could lead to someone accessing your files inappropriately, which could lead to a breach of confidentiality, for which, you would be accountable.

Do not leave patient's health records unattended, especially in public areas.

Do not download patient identifiable information from the Trust systems, or any other personal information for that matter, onto another computer system unless you are authorised to do so, by the Caldicott Guardian and Head of Health Informatics.

Ensure all information recorded on computer systems or paper based records is accurate. All information must be, to the best of your knowledge, accurate and up-to-date. If you are unsure of whether data is accurate, check with the person providing the information. All staff have a legal responsibility to ensure that the information they supply is accurate. (General Data Protection Regulation)

Do not access information about yourself, your relatives or friends. You

do not have an automatic right to such information, you should request access to your information via the 'subject access' route. Contact the Records Manager for an access form.

Do not give confidential information over the 'phone or via fax without first checking the identity and authority of the caller/receiver. There will be an agreed procedure for doing this. Check the fax number is correct, send a single sheet fax initially, and check that it has been received at the other end (and vice versa). If you must send confidential information via a fax, ensure some one is there to receive it and be sure that it will not 'sit' on the fax machine for more than five minutes. Confidential information should not be routinely given over the telephone - how do you know the person is who they say they are, particularly if it is an unknown person and do you have clear authorisation to release the information? Follow the **"Safe Haven Policy."** It will identify methods whereby such information can be transferred by fax or 'phone in the knowledge that there is a person authorised to receive the information at the other end of the line.

Do not put confidential waste into the normal waste bin. Consider shredding the documentation. If shredding on-site is not an option, how do you ensure that the information is stored securely until such time as it is disposed of? Do you know your organisation's policy?

Ensure confidential notes are placed in sealed envelopes if sending through the (internal or external) post. Ensuring the address is correct, clearly written and marked confidential, for addressee only. Consider the use of recorded delivery. This allows an audit if the records do go astray. What is that organisation's policy for protecting the information?

Do not speak about patients in public areas or where 'unauthorised people' can overhear - Don't use patient names when speaking about patients in public areas, on the telephone, unless you are sure you cannot be overheard.

As laid down in the Terms and Conditions of Employment any breach of confidentiality may lead to disciplinary action being taken.

Finally, do not hesitate to seek advice when you need it.

People who can help you:

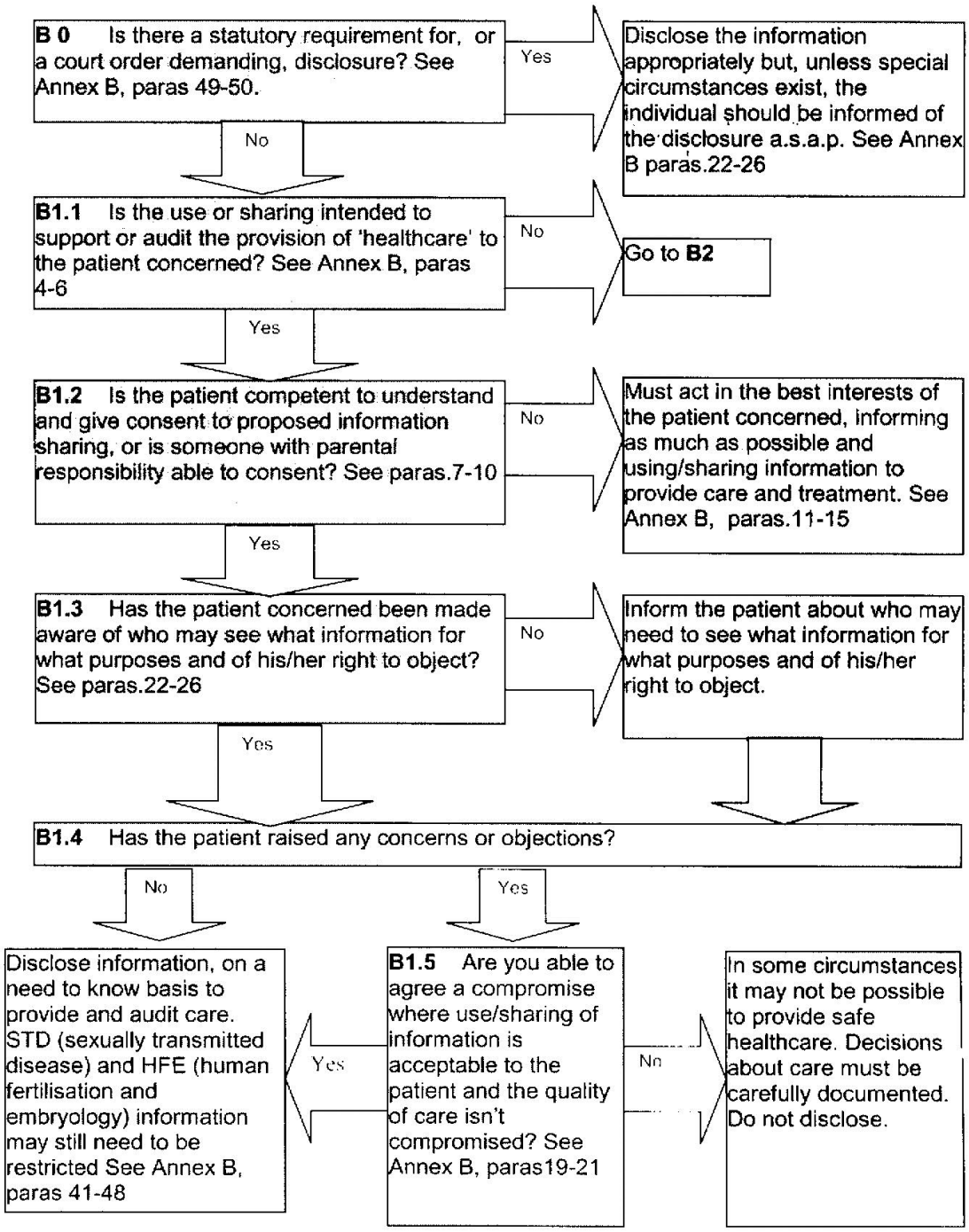
Your Manager

The Caldicott Guardian.

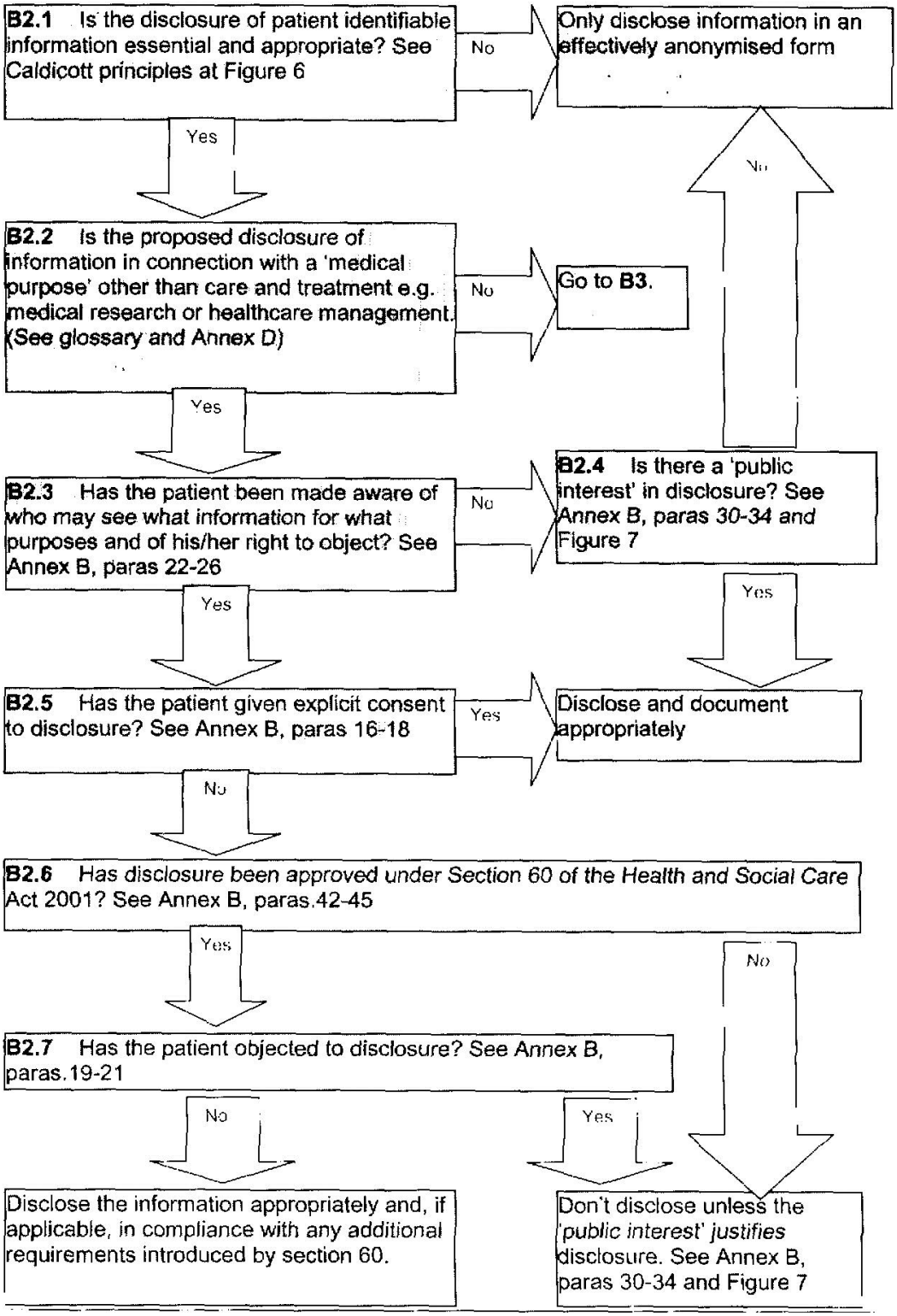
Officer with Delegated Caldicott Responsibility.

NHS Models for the Disclosure of Personal Information

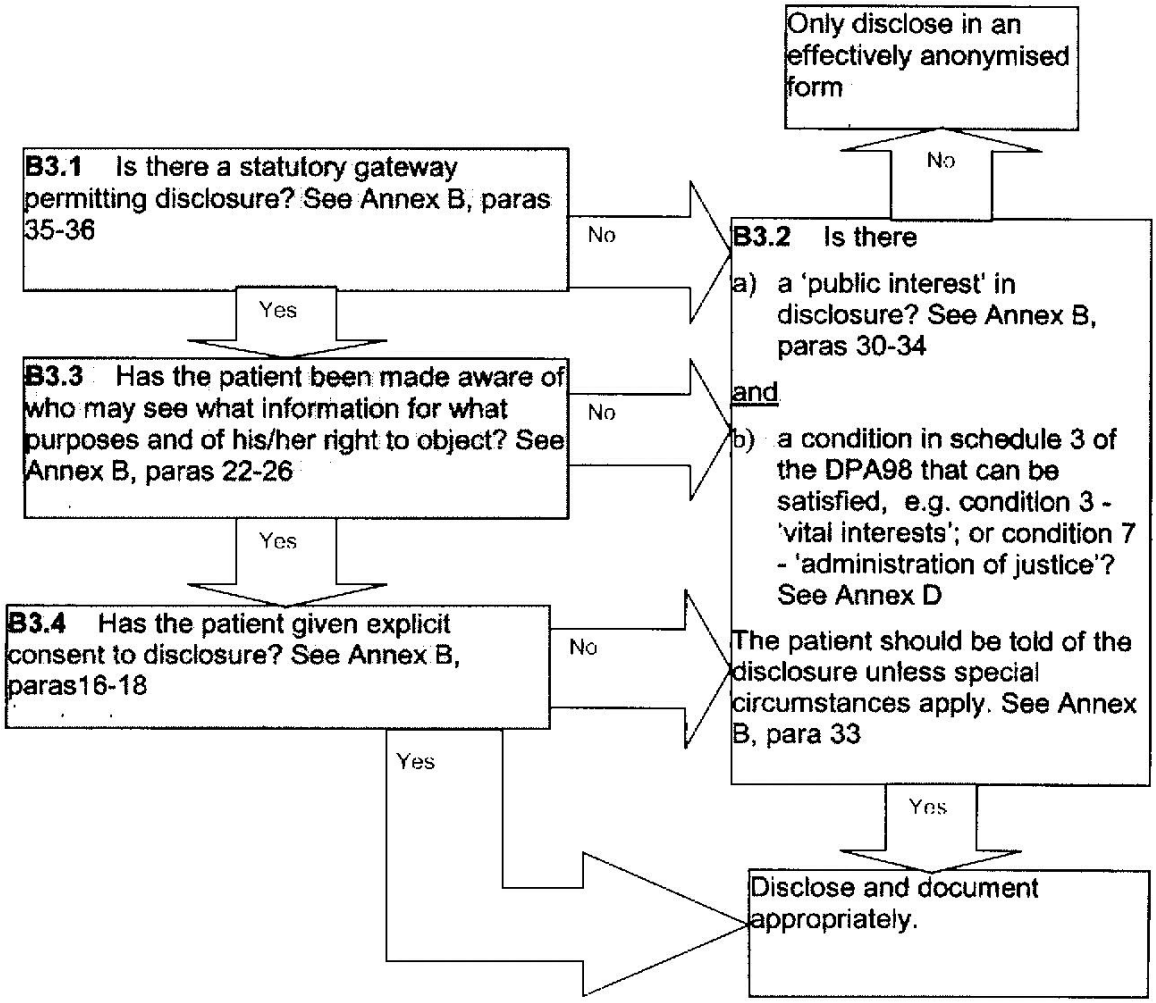
B1: Disclosure Model[11] - where it is proposed to share confidential information in order to provide healthcare



B2: Disclosure Model - where the purpose isn't healthcare but it is a medical purpose as defined in the legislation



B3: Disclosure Model - where the purpose is unrelated to healthcare or another medical purpose



APPENDIX 5

Guidance for the Confidentiality of Staff and other Personal Information

Introduction

The General Data Protection Regulation, the Common Law Duty of Confidentiality, and the Human Rights Act 1998 all apply equally to personal information of any description, not just Health Records. As a result, staff records, contractor records and any other personal information held by the organisation has to be kept and used for legitimate and limited purposes, as described under the General Data Protection Regulation

All subjects of information should be aware of the nature of the information held about them and the reasons for holding such information. The information, whether computer held or held in manual filing cabinets should be kept secure and in such a way that it cannot be accessed by anyone other than an authorised person.

Personal Information

Whilst not exhaustive the following information is typically that which would be held in staff or contractor records and which could be seen as being subject to the Data Protection Regulations.

- Staff employment history
- Details of disciplinary hearings
- Pay and taxation
- Training Records
- Demographics
- References
- Occupational Health
- Criminal Record Bureau

Some of this information is more sensitive than other information.

At any time someone may ask to see their records and as with all other records is one month in which to present that information. There are no exemptions and should incorrect information have been recorded, then there is a requirement to erase, destroy or correct the information. Should someone have suffered financially as a result of incorrect information having been recorded, then they are entitled to compensation under the General Data Protection Regulation.

References

References can be thought of as the most controversial of all staff documents since they are often based on subjective and opinionated comments on the

part of the author. Sometimes it could be difficult to substantiate the comments.

As a result, anyone writing references on behalf of the trust will follow HR advice and ensure that they stick purely to factual comments which can be backed up with further documentation, if necessary. By way of guidance, assume everything written about the data subject and which appears in the staff will at some time be seen by the data subject.

Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any procedural document that requires ratification

	Title of document being reviewed:	Yes/No	Comments
1.	**Title**		
	Is the title clear and unambiguous? It should not start with the word policy.	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**	Yes	
	Are reasons for development of the document stated? This should be in the purpose section.	Yes	
3.	**Development Process**		
	Does the policy adhere to the Trust policy format?	Yes	
	Is the method described in brief? This should be in the introduction or purpose.	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
	Are all terms clearly explained/defined?	Yes	
5.	**Evidence Base**		
	Has a comprehensive literature search been conducted to identify best evidence to inform the policy?	Yes	
	Have the literature search results been evaluated and key documents identified?	Yes	
	Have the key documents been critically appraised?	Yes	
	Are key documents cited within the policy?	Yes	
	Are cited documents referenced?	Yes	

	Title of document being reviewed:	Yes/No	Comments
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	No	
	For Trust wide policies has the appropriate Executive lead approved the policy?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**	Yes	
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?	Yes	

Reviewer			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name		Date	
Signature		Approving Committee/s	IGSG/Policies and Procedures Group and Trust Executive Committee

Lead Manager (Local Policies) / Director (Trust Wide Policies)			
If you are assured that the correct procedure has been followed for the consultation of this policy, sign and date it and forward to the Compliance and Risk Department for ratification.			
Name	Corporate Governance Manager	Date	May 2018
Signature		Approving Committee/s	IGSG/Policies and Procedures Group and Trust Executive Committee
Ratification Committee Approval			
Quality Board minute number: PPG minute number: **TMB minute number:**			

Service Overview & Improvement Action Plan: Equality Analysis Form

Title: Confidentiality Policy	What are the intended outcomes of this work? The purpose of this policy is to outline the principles related to confidentiality and to support staff in applying these principles.
Who will be affected? All staff	Evidence: N/A

ANALYSIS SUMMARY: considering the above evidence, please summarise the impact of the work based on the Public Sector equality duty outcomes against the 9 Protected characteristics			
Public Sector Duty *Protected Characteristics* (highlight as appropriate)	**Eliminate discrimination, harassment and victimisation**	**Advance equality of opportunity**	**Promote good relations between groups**
AGE / DISABILITY/ RACE	*This may refer to vulnerable adults and vulnerable safeguarding children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
SEX (Gender)/ GENDER REASSIGNMENT	*Refer to Gender Recognition Act 2004*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality*	*The General Data Protection Regulation will promote positive relations between all groups.*

		of opportunity to all groups.	
RELIGION or BELIEF/ SEXUAL ORIENTATION	*This may refer to vulnerable adults and vulnerable safeguard children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
PREGNANCY & MATERNITY	*This may refer to vulnerable adults and vulnerable safeguarding children*	*The General Data Protection Regulations includes provisions that promote accountability and governance and as such Walsall Healthcare NHS Trust has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to promote equality of opportunity to all groups.*	*The General Data Protection Regulation will promote positive relations between all groups.*
MARRIAGE & CIVIL PARTNERSHIP	*No impact*	*Not applicable at present*	*Not applicable at present*

What is the overall impact? There are no negative implications associated with this policy. The implementation promotes positive opportunities and relationships between all groups and is in accordance with the new General Data Protection Regulations.

Any action required on the impact on equalities? *Impact of this policy has been assessed and it will not lead to any discrimination or other adverse events on any population groups, as described above.*

Name of person completing analysis	*Corporate Governance Manager*	**Date completed**	*May 2018*
Name of responsible Director	*Director of Strategy and Improvement*		
Signature			