# Data Protection and
# Code of Confidentiality Policy

| | |
|---|---|
| Policy / procedure code: | IG002 Data Protection & Confidentiality Policy |
| Version: | 1.1 |
| Ratified by: | Corporate Governance Committee |
| Name of policy owner: | SIRO (Director of Finance) |
| For Information and action to: | All WSBH staff |
| Name of originator / author: | B Hamilton |
| Reviewed: | January 2018 |
| Issue date: | February 2015 |
| Next review date: | May 2021 |

**Version Control Sheet**
**Policy: Data Protection and Confidentiality Policy**

| Version | Date | Author | Status | Comment |
|---|---|---|---|---|
| 1.1 | Nov 2017 | B. Hamilton | | Major review – incorporate organization wide standards and GDPR references |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Signature Sheet: Policy: Data Protection and Confidentiality Policy Code:**

| Date | Name | Designation / Post | Department | Signature |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Contents

## 1. Introduction

The key legal documents covering security and confidentiality of personal confidential information are the General Data Protection Regulation [GDPR ] (2018); The Data Protection Act [DPA] (1998); NHS Confidentiality Code of Practice (2003); The Human Rights Act (1988); Freedom of Information Act (2000); The Common Law Duty of Confidence and Caldicott Review recommendations(2013). Additionally WSBH must adhere to NHS confidentiality and information security standards; Department of Health (DOH) guidance and professional body guidance. Private and Third Sector organisations must act only within their statutory powers. In addition Privacy Impact Assessments (PIA) are now mandatory for any new system, process or procedure (IT or otherwise) that involves Personal Confidential Data (PCD). *( See Organisational Change Policy IG06 and Privacy Impact Assessment Policy IG07)*

WSBH holds and processes information about its patients, staff and other individuals in order to carry out the business as a charity provider of healthcare services. Primarily personal confidential information collected verbally, manually or electronically must be processed fairly, stored securely and disclosed lawfully (*See Appendix 1 for a summary of the DPA principles.)*

**The successful implementation of the Date Protection and Confidentiality Policy is dependant on organisation wide awareness raising and continual monitoring of employees understanding of the application of data protection and GDPR standards .** Failure of the WSBH or its staff (including contractors and volunteers) to comply with legislation may well result in investigation and may risk the imposition of substantial fines (up to £500,000) by the Information Commissioners Office (ICO).

**NB:** The Data Protection Act 1998 is superseded by the introduction of the EU General Data Protection Regulation (GDPR) on 25th May 2018. GDPR will strengthen and extend current Data Protection law. The principles will be similar to those in the Data Protection Act 1998. The most significant addition to GDPR is a new organisational accountability requirement.

## 2. Scope and Purpose

- This policy applies to all WSBH organisational activities (Fund raising, Human Resources, Healthcare).
- This policy apples to everyone working for or on behalf of WSBH working with personal confidential or sensitive data including bank staff, agency/locum workers and those working for the organisation in a voluntary or honorary capacity. This includes contractors and employees of partner agencies where contractual arrangements are in place.
- The policy applies to verbal, written and electronic information acquired directly or indirectly and processed by WSBH.
- All staff (clinical and non-clinical) must ensure that all patients, staff and other personal confidential data held by WSBH remains confidential and they comply with the requirements of the Data Protection Act 1998 and the General Data Protection Regulation (2018).

The purpose of this policy is to:

- Ensure WSBH complies with legislation, meets statutory obligations and observes high standards of information governance practice and ensure personal and sensitive confidential data is dealt with legally, securely, effectively and efficiently, in order to maintain safe quality service.

- Ensure patients, carers and public are provided with information about their legal rights to be informed about how their data is stored securely, used and shared.
- Emphasise the duty to share information can be as important as the duty to protect patient confidentiality.
- Highlight staff responsibilities under current legislation and the WSBH Information Governance Framework.
- Define standards for information sharing personal and non-personal (business) information.
- Minimise risks of information security breaches, prosecution and financial or reputational penalties.

### 3. Conditions required for processing Personal Sensitive Data

To process sensitive personal data *(See appendix 6 for definitions)* at least one of the conditions relating to fair processing set out in Schedule 2 to the DPA and at least one condition from Schedule 3 must be satisfied. These include the following conditions:

- With **explicit consent** of the data subject
- Where there is a legal obligation on the data processor to do so in relation to employment
- Where it is necessary to protect the vital interests of the data subject and the data controller (WSBH) cannot reasonably obtain consent and consent cannot otherwise be reasonably obtained
- Where a not-for-profit organisation existing for political, philosophical, religious or trade union purposes processes in the course of its legitimate activities and relates only to individuals who either are members of the body or association or have regular contact with it (N.B. it is doubtful whether many charities fall within this)
- Where information has been made public by the deliberate steps of the data subject
- Where processing forms a necessary part of legal proceedings, is necessary for obtaining legal advice, or for establishing, exercising or defending legal rights
- Where the processing is necessary for the administration of justice or House of Parliament functions
- Where processing is necessary for medical purposes and is undertaken by a health professional
- Where processing is necessary for monitoring equal opportunities
- In the course of legitimate political activities, or research activities that are in the substantial public interest or where the personal data must be processed in circumstances specified by the Lord Chancellor

### 4. Individuals' (Data Subjects) Rights

The 6th data protection principle covers the rights of individuals in relation to their individual data:

- A right of access to a copy of the information comprised of their personal data within 21 working days
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- A right to claim compensation for damages caused by a breach of the DPA.
- WSBH must stop processing or prevent processing;
  - Where it can be shown that processing data is likely to cause substantial damage or distress and that

may damage or distress is, or would be, unwarranted
  - for the purposes of direct marketing when asked to stop
- WSBH must refrain from decisions made automatically (without human involvement). *Listed exceptions to this can be obtained from the ICO, although it is unlikely these will apply to fundraising.*

## 5 Uses of Personal Sensitive Data for Non-healthcare services

**Fundraising** (The Fundraising Regulator)The DPA 1998 and GDPR 2018 set out requirements for those processing "sensitive personal data", which includes information about a person's ethnicity, religion, sexuality, political beliefs, trade union membership, criminal record and health condition.
Personal data must not be processed unless the data controller (WSBH) has notified/registered with the Information Commissioner.
To comply with the Data Protection Act 1998, processing must observe: Data Protection Principles; data subjects' rights; and must be consistent with the data controller's notification. *See Appendix 1 Data Protection Principles*

### 5.1 Consent

Consent is one of the most frequently relied upon conditions for fair processing and appears both in relation to processing personal data and sensitive personal data (which requires explicit consent) for fundraising purposes. There is no definition of "consent" contained within the Data Protection Act. However the following principles apply:

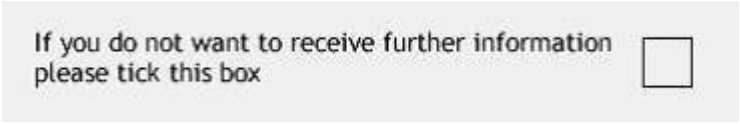
- If sensitive data is being processed, explicit consent or Opt In Opt Out choices must be obtained.
- WSBH must give the collection of data careful consideration.
- Donors / contacts must not be misled or deceived as to how their information will be used and how the organisation may contact them in future.
- If a donor or contact informs an organisation that they do not wish to be subject to direct marketing, then the organisation must comply with that request.
- If the organisation is part of a group and requires the right to pass personal data to trading subsidiaries or other entities within the group, each entity within the group is considered a separate data controller (unless they are acting as a data processor on behalf of the organisation).
- The organisation must ensure that data subjects are informed that their information may be shared with the trading subsidiary if such sharing is likely to take place at the point of data capture
- When researching individuals, it is unlikely you will need consent to processing sensitive information relating to them if using information already in the public domain.

### 5.2. Opt-In and Opt-out

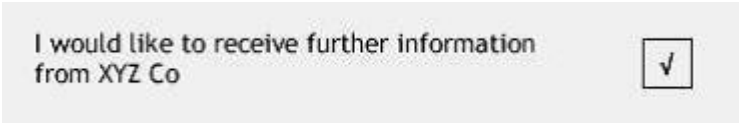
- When collecting personal data, it is important to consider whether or not you would like to contact them again in the future and by what means. It is necessary to obtain the consent of an individual if they are to receive unsolicited direct marketing by electronic means in the future.
- Organisations seeking consent for third parties to contact the individual ought to be clear about the data that will be shared and how it will be used. If an organisation is seeking consent on behalf of the third party for the third party to send marketing to the individual, it should make this clear and seek legal advice where necessary about an appropriate form of words.
- **Opt-In:** For direct marketing by email or SMS to individuals, or by fax to individuals or which uses an automated calling system, it is necessary to get the data subject to consent to such marketing . e.g. "If you would like to receive further marketing information from us about our work by email, please tick

this box…"

- **Opt-Out:** For direct marketing by post, fax (between two companies), and telephone, consent is not needed, but organisations MUST include an opt-out statement.g.




- Alternatively, where information is being collected online, it is possible to have a statement with the customer being required to opt-out by un-ticking the box:




- **Soft Opt-In:** If consent has not been obtained, the only way in which direct marketing may be sent by electronic email or SMS to individuals, under an automated calling system, is if the so called "soft opt-in" provisions are met, that is:
  - The recipient's e-mail address (or a mobile number in relation to texts) was collected in the course of a sale or negotiations for a sale (where an individual has actively expressed interest in an organisation's products or services and has not opted out of further contact)
  - The sender only sends promotional material relating to their similar products and services
  - At address collection, the recipient was given the opportunity to opt-out, which wasn't taken.
- The opportunity to opt-out MUST* be given with every subsequent message.
- A donation from an individual would not constitute a sale and so the 'soft opt-in' would not be relevant for ordinary fundraising. The 'soft opt-in' would be relevant if an organisation's commercial goods and services were being promoted.

### 5.3 Privacy and Electronic Communications (EC Directive) Regulations, 2003 As Amended

Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the Regulations") has been produced by the ICO.

- The Regulations cover registrations with the Telephone Preference Service and the sending of unsolicited direct marketing material using the telephone, fax or electronic communication methods including e-mail and text/video/picture messaging.
- "Direct Marketing" refers to the communication of advertising or marketing materials to particular individuals, and includes the sale of goods and services and the promotion of an organisation's aims and ideals.

### 5.4 Telephone

- WSBH must require that any agency or third party that they work with complies with the requirements of the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 including the requirements of the Telephone Preference Service, regardless of the country or legal jurisdiction in which the agency is based or operating. In some circumstances this is a legal requirement for charities, but in other circumstances it may not be.
- Three different possible legal scenarios could apply here:
  - It is a legal requirement for charities to ensure that agencies and third parties who are processing personal data on their behalf as data processors, wherever they are based, comply with the Data Protection Act 1998.
  - Where an agency or third party is working with a charity but processing personal data for the

agency or third party's own purposes as a data controller, whether or not compliance with the Data Protection Act 1998 or other similar legislation is a legal requirement for that agency or third party will depend on where the agency or third party is located and whether the agency or third party uses equipment in the UK. In any event it will not be a legal requirement for the charity to ensure that the agency or third party is compliant (except where the agency or third party is also acting as a data processor for the charity – see paragraph 1 above). However, if the charity is transferring personal data to the agency or third party, it must ensure that this transfer is in accordance with what it has told the supporters whose data is transferring about how their personal data will be used.

- Whether compliance with the Privacy and Electronic Communications (EC Directive) Regulations 2003 is required by law where an agency or third party is based overseas will depend on whether 'use' of the telephone service is held to have occurred in the UK.

- Data protection law in relation to transfers of data outside of the EU is a complex area of law, and there are other legal requirements in the Data Protection Act 1998 which are not re-stated here as they are beyond the scope of the Code. Charities should seek legal advice on their specific arrangements if they are unsure whether there is a legal requirement for any agencies or third parties they use to comply with this legislation.

**5.5 Electronic Mail**

- The Regulations relating to electronic mail refer to e-mail and text/picture/video marketing messages and the Information Commission also considers voicemail, answerphone messages and social networking messages to be included.
- WSBH must not conceal their identity when sending marketing messages electronicaly.
- WSBH must provide a valid address for opt-out requests.
- WSBH must not send unsolicited marketing material by electronic means to individual subscribers unless the recipient has previously consented to receiving such material
- An individual subscriber is a living individual and includes an unincorporated body of such individuals. It therefore means a residential subscriber, sole trader or unincorporated partnership in England, Wales, Scotland and N Ireland.

**5.6 Keeping data**

- The fifth data DPA principle requires that personal data must not be kept longer than is necessary.
- This means that data that is being processed for a particular purpose must not be kept unless it is still required for that purpose.
- WSBH must maintain a 'suppression list' (containing details of individuals who have asked not to receive direct marketing material) and always check this against lists for direct marketing.
- Before deleting any information it is important to consider whether there are any other legal requirements that mean certain elements of the data need to be retained.

**5.7 Exchanging Lists**

- If personal data is captured from any source other than from the data subject, the data controller (WSBH) must ensure that the data subject has been given information regarding the identity of the data controller (WSBH), the purpose of the processing and any other relevant information unless one of a limited number of exemptions set out in the Data Protection Act 1998 applies.
- There is a possible exemption from this obligation if it would entail "disproportionate effort" or if it is

"not practicable" for the organisation for any of these reasons:

- The cost to the data controller
- The time (and therefore cost) it would take
- The ease with which that information could be provided, set against the degree of harm or concern that non-provision of the data might have. Any doubts around this complex area ought to be raised and clarified with the ICO.

## 6. Uses of Personal / Sensitive Data for Healthcare Purposes

All uses of patient information must comply with the DPA, GDPR and Caldicott principles. Healthcare purposes include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of healthcare provided including:

### 6.1 Clinical service delivery

### 6.2 Clinical audit

is usually conducted by those involved in patient care. If a patient does object it should be explained why the information is needed and how this may benefit their own, and others' care. If it is not possible to provide safe care without disclosing information for audit, an explanation must be provided to the patient including the options open to them. (GMC: Confidentiality Guidance, Protecting and Providing Information. 2009). Where an audit is undertaken by the clinical team providing care, or those working to support them (clinical administrators) patient identifiable information may be used assuming implied consent provided that patients have been informed (WSBH Privacy / Fair Processing notice , patient leaflets) that their data may be used for this purpose and have not objected.

### 6.3 Clinical Research

is usually conducted with explicit patient consent or approved (under section 251 of the National Health Service Act 2006) by the Health Research Authority or local Research Group. The use of patient identifiable information for research usually requires explicit informed patient consent.

- When seeking consent for disclosure, patients must be given enough information to allow them to make a considered and informed decision.
- Specifically, they should be informed of the reasons for the disclosure, the way that it will be made and the possible consequences. The exact amount of disclosure and the identity of those who will receive it should also be explained.
- If a patient cannot be contacted to give consent, it should not be assumed that their medical details can be used for research purposes.

### 6.4 Clinical Service evaluation

includes activities to evaluate and improve services. Minimal patient identifiable information may be used providing the principles below are strictly followed:

- The purpose of the processing must be covered by the WSBH Privacy /Fair Processing Notice
- The purpose of the processing must be approved in advance by the SIRO & Caldicott Guardian.
- Anonymised or pseudonymised data should be used where possible. Where pseudonymised data is used the key must be known only to minimal numbers of staff. Use of any identifiable data must be justified.
- Where personal data is justified, e.g. to follow a specific patient through a pathway, only process the minimum personal data required to fulfil the purpose, e.g. NHS number. The data collected must not be used for a different purpose without further authorisation.
- Outputs, e.g. reports, from service improvement/evaluation activities should be anonymised unless use of personal data can be justified.

- Access to personal data for service improvement/evaluation activities is restricted only to WSBH staff who need to process it.
- Personal data must be stored and transferred securely, and disposed of securely when no longer required.
- Data repositories (e.g. spreadsheets/databases containing personal data must be registered in the Data Purpose Log.
- All staff with access to personal data must be up-to-date with their Information Governance training.

### 6.5 Clinical Training

- Use of patient information is essential to the education and training of healthcare professionals. For the majority of uses anonymised information is sufficient and must be used whenever practical.
- Most patients understand and accept that the education and training of medical and other healthcare students and trainees relies on their having access to information about patients. (The Privacy /Fair Processing Notice) and patient leaflets makes this clear.
- Where trainee clinicians are part of the team providing or supporting a patient's care they can access relevant personal sensitive data with the patient's consent. The lead clinician has responsibility for obtaining this and recording within the medical record and ensuring that the patient is under no pressure to consent.
- WSBH staff must request and document patients' informed consent prior to making any audio or recordings for training purposes to ensure compliance with the Data Protection Act.

## 7. Financial Audit and Management

- Personal confidential information shared for non-healthcare purposes requires the purpose for sharing to be defined and limited, and additional requirements such as recorded informed consent of evidence of support may be required to enable lawful sharing.
- When sharing for non-healthcare purposes including commissioning, healthcare development, improving efficiency HSCIC Secondary use Services Guidance must be complied with.

## 8. Systems Testing and Personal data

- The ICO advises that the use of actual personal data for system testing should be avoided.
- Where there is no practical alternative to using live data for this purpose, systems administrators should develop alternative methods of system testing.
- Should the ICO receive a complaint about the use of personal data for system testing, staff must be able to justify why no alternative to the use of live data was found.

## 9. Human Resources

- The HR department will keep and maintain employee manual and computerised files on all employees including bank staff and ex-employees. The sole purpose for which personal data will be processed will be for personnel administration and reporting purposes. Personal employee data will be processed fairly and lawfully and will not be processed unless the employee has given their consent or it is necessary for the performance of contract. Personal employee data will be accurate, adequate, relevant and not excessive in relation to the purposes for which it is being processed. Personal employee data will not be kept longer than is necessary.

- Access to the manual personnel files will be restricted to the Executive Team and senior management.
- Manual personnel files must not be removed from the HR department without prior permission from the HR Director.
- The introduction of a new HR computer system will allow managers to access certain records. HR will ensure access codes are set up to ensure appropriate records and levels of authority are maintained.
- Data kept on manual files and or the HR computer system will include, but not limited to:
  - application form or CV
  - references
  - contracts of employment
  - occupational health clearance
  - any discipline or grievance records (expired warnings will be destroyed)
  - appraisal forms
  - salary details
  - benefit details
  - absence data (including self certification forms and Doctor Fit Note Certificates)
  - training records
- Employees are allowed to have access to all personal data held about them. Employees should make their request in writing to the HR Director. Please refer to the Privacy Notice for more information.
- The retention of HR information:
- Application forms and interview notes (for those interviewed but were unsuccessful)
- 6 months.
  - Application forms of those not shortlisted
  - 1 month (unless there may be other roles which the manager feels they could be suitable for in future and then they will kept them for 6 months)
  - Personnel files
  - 6 years after employment ceases.

## 10. Responsibilities

**Chief Executive and Executive Board:** have overall responsibility for ensuring robust operational management systems and governance are in place in order for WSBH to be able to comply with the Data Protection Act 1998, The GDPR (2018) and the general law on matters of confidentiality.

**The Chief Executive** has the ultimate responsibility for compliance with the Data Protection Act 1998 and GDPR (2018) for the confidential information held and ensures WSBH directors:

- Continually improve on compliance with IG legal and best practice guidance
- Fully observe conditions regarding the fair processing of information
- Meet legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality and integrity of information used.
- Ensure data subject rights can be fully exercised including the right:
  - To be informed that processing is being undertaken
  - To be made aware processes are in place to access their personal information
  - To prevent processing in certain circumstances
  - To rectify, block or erase information which is regarded as factually inaccurate information

- To be assured appropriate technical and organisational security measures are in place to safeguard personal information
- To be assured that personal sensitive data is not transferred abroad without suitable safeguards

**Senior Information Risk Owner (SIRO)** – an executive director responsible for:

- Strengthening controls around information governance and security
- Ownership of the organisation's IG risk register and risk assessment process
- Providing advice to the Accountable Officer on the the Statement of Internal Control (information risk).
- Ensuring an effective information assurance governance infrastructure is in place including information asset ownership, Caldicott Guardianship, reporting, defined roles and responsibilities and quality assurance of all records.
- Providing a report to the Accountable Officer and Executive Board regarding the information risk/security content of the annual Statement of Internal Control (SIC) and annual report.
- Chair the Information Governance : Toolkit Committee.
- Authorise IG Toolkit Self-Assessment submissions.

**Data Protection Officer**:

- Maintains WSBH Data Protection registration with the Information Commissioner's Office
- Leads on the data protection work programme in collaboration with the Caldicott Guardian.
- Advises on the options for lawful and ethical processing of information.

**Caldicott Guardian:**

- The Medical Director is the WSBH Caldicott Guardian leading on all aspects of Caldicott work as required by the Caldicott principles and the principles contained within the NHS Code of Practice (Confidentiality) *See Appendix 5*
- Ensures staff are made aware of individual responsibilities through policy, procedure and training.
- Provides advice as required on Data Protection and Caldicott issues and oversight of applications for disclosure of personal information.

**The Information Governance (IG): Toolkit Committee**

- Is chaired by the WSBH SIRO and responsibilities include:
  - The Information Governance Toolkit self-assessment
  - Raising awareness of IG and promote a healthy IG culture
  - Driving the Information Governance improvement agenda and annual Information Governance Improvement Action Plan
  - Provision of a monthly reports to the Corporate Governance Committee on Caldicott and Data Protection matters for wider communication
  - Approval of PIAs before the introduction of new information processes
  - Review and management of the IG risk register
  - Management of a standardised approach to obtaining consent for disclosure
  - Review action plans related to management of information security breaches and ensuring the resolution and ensuring lessons are learned and changes in practice occur.
  - Provision of regular IG Toolkit progress reports and an annual report to the Corporate Governance Committee.
  - Review, revise and ratify IG Policy.

**Corporate Governance Committee**

- Oversee IG standards and compliance
- Oversee day to day IG issues including incidents, audits and risks
- Oversee the annual IG Toolkit Action Plan

**IT Manager ( IT security and governance):**

- Ensure effective information governance technical infrastructure is in place including information asset ownership, flow mapping, reporting, defined roles and responsibilities
- Ensure, with the SIRO, that Information Asset Owners (IAOs) are nominated to manage local responsibilities under DPA 1988 & GDPR 2018 within their work area
- Maintain the WSBH's Data flow maps and Data Purpose Log.
- Maintain a register of all IT applications / databases containing Personal Confidential Data (PCD)
- Collaborate in assessment of Privacy Impact Assessments in relation to process changes to ensure new processes maintain the confidentiality, integrity an accessibility of information
- Provide expert technical advice on matters relating to IT Security and assure compliance
- Provide advice and support on data protection and information security breaches

**WSBH Business Manager**

- Maintain the WSBH's Information Sharing Agreements (ISA)
- Ensure all third party contracts /contractors are complainat with DPA 1988 and GDpr 2018

**Quality and Audit Lead:**

- Maintain the Caldicott Guardian disclosure log
- Coordinate IG audits

**HR and Education Lead/ Practice development Team:**

- Maintain and update the Information Governance staff workbook (HR & PDT joint responsibility).
- Provide IG training through induction and on-going face to face or e-learning courses
- Maintain a record of training
- All contracts of employment include a data protection and general confidentiality clause.
- All staff will be made aware of their responsibilities through their Statement of Terms and Conditions.

**Heads of Departments/ Managers:**

- Ensure all staff managing and handling personal confidential data are appropriately trained to do so and appropriately supervised as required
- Ensure staff understand responsibility for reporting and acting on data protection and confidentiality breaches on Sentinel and have received appropriate training.
- Support investigations into confidentiality breaches or potential breaches with relevant IAOs/IAAs, ensure reports and action plans are presented to the Information and Corporate Governance Committees for monitoring of compliance
- Implement this policy within their area and ensuring staff attend/undertake training and are familiar with the standards required
- Undertake regular IG audits which are sent to the Quality and Audit Lead.
- Report on Sentinel and investigate any Personal Confidential Data (PCD) breaches within their area of responsibility

- Be aware of the reporting and management of Serious Information Breaches . *See WSBH Incident and Serious Incident Management Policy.*

**All Staff:** (including contractors and volunteers) –

- Have a duty to maintain the confidentiality of individulas' information. This duty is required and must be complied with (conferred and owned) by common law, statute of law, contract of employment, disciplinary codes and policies (of which this is one) and professional registration.
- Are subject to an obligation of confidentiality and must adhere to the Data Protection Act, The GDPR 2018, Code of Confidentiality and Caldicott guideline professional codes of conduct and responsible for:
  - Undertaking training as identified by their line managers as required for their role
  - Ensuring they are familiar with the IG Handbook contents
  - Ensuring they are aware of the rights of individuals in relation to what information is held about them, how it is processed and their rights to access their information.
  - Ensuring they are aware of their personal responsibilities for data protection and confidentiality as a general staff member and/or an Information Asset owner/processor
  - Know how to avoid information security breaches
  - Know how to obtain support and advice concerning disclosure requests
  - Know how to report and respond to incidents where security of PCD has been breached.
  - Be aware that regular reviews and audits are carried out in respect of the way personal confidential data is managed; participate in audits and implement changes to improve data protection.
  - Understand their responsibility for reporting data protection and confidentiality breaches on Sentinel.

**Information Asset Owners (IAO's)** – responsible for:

- Accountable to the SIRO for providing assurance on the security and use of the information assets within their respective area are identified, recorded and controls are in place to mitigate any risks
- Support the SIRO in the overall information risk management function
- Identify, understand and address risk to the information assets they "own"
- Responsible for operational management of WSBH records according to policy
- Complete and maintain WSBH Information Asset Register
- Responsible for appointing Information Asset Administrators (IAAs). Working with IAAs to ensure they share a clear understanding of responsibilities and accountabilities relating to asset ownership. Especially vital where information assets are shared by multiple parts of the WSBH.
- Ensure actual or potential breaches of confidentiality are reported on Sentinel and investigated to ensure lessons are learned and changes in practice occur.

**Information Asset Administrators (IAA's):**

- Support I.A.O in the delivery of their information risk management responsibilities.
- Ensure policies and procedures are followed
- Recognise actual or potential security incidents and mitigate those risks
- Consult their IAO on incident management
- Ensure information asset registers are accurate
- Undertake follow-up reviews of failed log-in reports within their systems and reporting failures to their line management and on Sentinel

- Ensure security risks are controlled, risk assessments are in place detailing control measures and that these are regularly reviewed

## 11. Protecting Personal Sensitivel Data (PSD)

### 11.1 Informing patients and service users about 'how we use your data'

- WSBH is required to inform service users about how their personal information will be managed.
- There is a comprehensive patient information leaflet that details management of personal information that is widely available and a Privacy (Fair Processing) Notice on the WSBH external facing website.
- Improving communication with service users is continually monitored as part of the Information Governance Toolkit requirements

### 11.2 Securing your work area

The following standards apply:

- Administrative areas have limited access to authorised staff.
- Ground floor rooms should have locks on all windows and security checking implemented after hours.
- All areas holding data conform to health and safety requirements in terms of fire, flood, theft or environmental damage.
- Manual paper records containing personal sensitive data is stored in locked cabinets / rooms when not in use.
- Computer screens must be facing away from public view.
- Computers should not be left on view, or accessible to unauthorised staff. Staff must lock or log off when leaving their computer. A system to ensure automatic lock after 5 mins and automatic log off after 6 hours will be enforced.
- Information containing PSCD must not be put on display in public areas e.g. test results, room lists on walls/windowsills.
- Whiteboards in public areas must not show the key to information put on them.
- Fax machines are one of the most common causes of confidentiality breaches, many are used by several different departments and people often collect faxes without checking all pages are for them, There is a high risk of information being seen by unauthorised persons. Therefore, fax transmission should be avoided wherever possible.
- Fax machines will be phased out but where a paper fax still exists they must be kept in a locked office, have a coded password and be turned off out of office hours (where practical).
- Ensure if faxing PCD to another organisation it will be received in a Safe Haven fax machine, in a secure area and designated to receive confidential information. Request the recipient confirms successful transmission.
- For 'e' fax, set a 'read' and 'receipt' request. Pre-programme numbers for regular recipients into the fax machine where possible and double check the number dialled/selected is correct before sending.
- Staff must never send faxes if:
- They know the information will not be seen/picked up immediately.
- At times outside of the recipient's hours of work.
- Leave information unattended whilst a fax is being sent or received.

### 11.3 Unauthorised Access

- Information held by WSBH will only be accessed by authorised staff as required to carry out the course of their duties.
- Staff will only access the minimum information necessary for service management consistent with their WSBH duties.
- Staff will not look up or access information relating to themselves, family members, other relatives, friends, neighbours, public figures/celebrities or patients not under their care.
-

### 11.4 Safe Transfer of Information

**Communication by Post**

- Paper communication containing PCSD must be transferred in a sealed envelope and addressed by name to the recipient. They must be clearly marked "Personal and Confidential – To be opened by recipient only".
- When using window envelopes, ensure that only the name and address are visible.
- Always ensure the information is being sent to the correct person (mail, email).
- An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know.
- PCSD contained in paper transfers must be limited to those details necessary for the recipient to carry out their role.

**Communication by e-mail**

- Unencrypted transfer of personal information by e-mail to patients is allowable with the informed consent of the data subject/patient. Informed consent must be recorded in the clinical / other record.
- If there is a need to send PCSD to other organisations for healthcare purposes on a regular basis, this must be done through the WSBH's secure e-mail. Alternatively, through NHS Mail.

**Verbal Communication**

- Care must be taken to ensure personal details are not overheard by staff/public/relatives who do not have a "need to know". Discussions should be held in private locations and not in public areas, staff common areas or lifts.
- If information must be shared by telephone, steps must be taken to ensure the recipient is properly identified:
- Take a phone number and double-check that it is the correct number for the individual/organisation.
- Check the individual/organisation has a legitimate right to the information
- Call them back.
- Messages containing PCD must not be left on answer machines, unless a password is required to access them. They should never be left on communal systems.

**Transporting Personal/ Sensitive information from one location to another**

- The movement of any type of personal identifiable information from one location to another requires careful consideration of the confidentiality and information security risks involved, as the loss of a record is a potential clinical and confidentiality risk.
- A common cause of data protection and confidentiality breech is leaving documents / diaries in areas around the workplace (toilets, dining rooms, library, enroute to community visits). Care must be taken to keep papers on you at all times if you have to carry documents containing PSD and pick them up when you leave an area.

- Effective Tracking and Retrieval must be in place and records accurately tracked in real time from WSBH premises to their destination and upon receipt when returned. Every effort must be made to return records to WSBH premises the same day.
- Where service requirements require personal / sensive data to be taken off site (Community Services) or where data is held at home (Counselling) a risk assessment needs to be undertaken and Caldicott Guardian approval sought.
- Appropriate measures must be taken to ensure that members of the family or visitors to the home cannot gain unauthorised access to records.
- Large quantities of records must be transported in durable, secure and tamper proof containers. It is acceptable for smaller quantities to be transported personally by hand within an enclosed briefcase or bag. Containers must be marked 'CONFIDENTIAL', 'PROPERTY OF WSBH'.
- Records transported in cars must never be left on display (e.g. passenger seats) or left in an unattended car. The car must be secured when parked.
- It is the responsibility of each Hospice department to provide appropriate transport containers and to observe the requirements of the Manual Handling Policy.
- With larger quantities of records transport arrangements should be by WSBH transport.

**Transfers of Personal Confidential Data Abroad**

- Principle 8 of the Data Protection Act 1998, governs transfers of personal data and requires that it is not transferred to countries outside the European Economic Area (EEA), unless that country has adequate level of protection for information and the rights of individuals.
- The Caldicott Guardian must be consulted where the transfer of PCD to countries outside the EEA is being considered/requested. Final approval will be in line with ICO best practice guidance.

**Use of Social Media**

- WSBH recognises that many staff share professional knowledge and experience with other professionals and acknowledges that staff can benefit in professional development through relevant social media. Nevertheless, WSBH has an obligation to protect its information assets and patients' privacy, and so has restricted access from WSBH resources to a limited number of social network sites.
- Official WSBH blogs and websites are managed by the WSBH's corporate communication team guided by local operating procedures. Staff outside the communications team are not authorised to communicate by any means on behalf of WSBH, unless approved in advance.
- Staff are ultimately responsible for their own online behaviour, but are advised not to divulge details of their employer within their personal profile page (i.e. in accordance with professional guidelines RCN,GMC).
- Staff must avoid online statements, posts or actions that are inaccurate, libellous, defamatory, harassment, threatening or may otherwise be illegal or bring the WSBH reputation into disrepute.
- Staff using social media privately, must not disclose WSBH information that is, or may be, sensitive/confidential, or that is subject to a non-disclosure contract. This includes information (written or photographic) about patients, colleagues, contractors, other organisations, commercial suppliers or WSBH business activities.
- Breaches will be investigated and result in disciplinary actions in accordance with WSBH policies and procedures, and has the potential to lead to civil or criminal proceedings against individuals.

## 12. Sharing of information (PCD)

- Under the Data Protection Act 1988, Human Rights Act, NHS, Caldicott Guidance and GDPR 2018, staff are under a duty of confidence to keep personal/sensitive information confidential and secure.
- Patient's retain the right to restrict disclosure of their personal information to other healthcare professionals or to relatives or carers. In these circumstances they should be encouraged to be very explicit about persons they do not want to access their information and this must be accurately recorded in their clinical records.
- There are, however, rare occasions where a patient's confidentiality may be overridden and this decision must only be made by the senior clinician involved at the time. Examples of these circumstances include:
  - Where the patient's life may be in danger, or the patient incapable of making an informed decision.
  - Where there is serious danger to others, or the rights of others may supersede those of the patient.
  - Where there is a serious threat to the healthcare professional.
  - Where there is a serious threat to the community.
- PCD can also be requested for disclosure by the Police, Social and Probation Services, under section 29(3) of the Data Protection Act 1998: Crime, Taxation and Fraud.
- Disclosures may be permitted, subject to application & approval under Section 251 of the NHS Act 2006.
- Decisions regarding disclosure of confidential information WSBH without the individuals consent must be taken by the Caldicott Guardian, and recorded in the Caldicott Log.
- Other occasions when WSBH will be bound to disclose confidential information without consent:
  - Birth and death notifications
  - Notifiable communicable diseases
  - Poisonings and serious accidents in the workplace
  - Terminations
  - Misuse of drugs
  - Safeguarding children and vulnerable adults
  - Road traffic accidents
  - Prevention / detection of a serious crime i.e. murder or terrorism.
  - Prior to disclosing information advice must be sought from your Line Manager and Caldicott Guardian.
- Factors to be considered when deciding to share personal / sensitive data or entering into data sharing agreements include:
  - What is the data sharing intended to achieve. There should be a clear objective /s
  - Could the objective/s be met without sharing personal data or by anonymising
  - Is the data to be shared limited to only that which is required to satisfy the objective. Use the minimum necessary
  - Who requires the data – use the 'need to know' priniciple when planning data sharing internally and externally
  - When should it be shared. The process and frequency must be fully documented
  - How should it be shared addresses the security of access and transmission
  - How idata sharing monitored – regular checks on the continued appropriateness of sharing must be carried out
  - How are individuals made aware that their data is being shared
  - Have the risks associated with data sharing been identified for all data flows

- Organisations achieving of level 2 or above on the NHS Operating Framework IGT requirements can be regarded as 'trusted organisations' for information sharing and sharing agreements are not required between them
- 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 the Caldicott principles supported by local, regulators and professional bodiy policy and guidance. The new Caldicott principle on information sharing (principle 7) confirms information sharing is legitimate

**12.1 Information Sharing Agreements(ISA)**

Before entering into any data sharing arrangements, it is good practice to carry out a Privacy Impact Assessment (See WSBH Impact Assessment Policy) which will assess the benefits that the information sharing might bring to specific individuals , organisations or society more widely. It will also help to assess risks or negative effects or likelihood of damage, distress, embarrassment being caused individuals or organisations.

- ISA are required for WSBH to manage and record the use and transfer of PCSD with partner agencies for purposes of continuing clinical care or other business reasons.
- The documents sets out:
  - The requirements for all signatory organisations to carry out responsible information sharing
  - The partners to the agreement are, potential recipients and the circumstances for access
  - The data controller and processors
  - The legal base of sharing
  - What information is to be shared and the purpose and methods of sharing
  - Necessary security arrangements
  - Data quality – accuracy, relevance, usability
  - Retention of shared data
  - Individual's rights
  - Review of effectiveness / termination date
  - All party obligations and stadards agreement
  - Sanctions for failure to comply.
- Any ISA must be approved by the IT Manager and Caldicott Guardian for each partner organisation.
- Any new data flows that arise out of a new project or procurement where WSBH is the data controller or receives personal, confidential, sensitive or business sensitive information will need to be recorded in the Information Asset Register.

**12.2 Third Party Contractors and SLA Agreements**

- Third parties may be granted access to WSBH information in a number of ways, and it is vital that the nature and level of access is risk assessed before confidentiality elements of contracts are drawn up.
- Third party access may be granted to WSBH systems and networks e.g. clinical system software may be maintained by the system suppliers under contract.
- In these cases it is most likely that the suppliers' staff may have substantial access to confidential data. Confidentiality and non-disclosure clauses must be included in the contract between the WSBH and system supplier.
- As part of the procurement process or contract renewal the Business Manager will investigate security controls in place with third party suppliers; including:
  - Are there adequate security controls, policies and training

- Are staff screened prior to employment
- Are they registered for data protection with the ICO

### 13. Data Protection Breach Reporting

- All data protection incidents are reported on Sentinel
- Data Protection Incidents are reviewed at Corporate Governence Committee
- The grading of Information Governance breaches and need for external reporting is covered in the Incident & Serious Incident Management Policy. See WSBH Incident & Serious Incident Management Policy

### 14 Mobile Devices / Photography

- All WSBH owned mobile devices have Mobile Device Management (MDM) software installed with the ability to control and track remotely and protect the data held. Users requesting to use their own device will be required to permit the installation of MDM.
- It is prohibited to use non-WSBH equipment or mobile devices (e.g mobile phone, tablet) to take patient images or to photograph information relating to a patient or their treatment.
- If it is deemed essential, with no other options available, images can be taken using an encrypted mobile device, however the device must not be synched to cloud services.
- Images must never be sent over a mobile phone network. The image must be deleted as soon as possible.
- There must be a fully justifiable purpose for a visual image to be carried out and consent must be obtained

### 15 Information Governance Training

- The successful implementation of the policy is dependant on organisation wide awareness raising and continual monitoring of employees understanding of confidentiality.
- All staff and volunteers must take and pass annual information governance training.
- WSBH has also developed in information handbook which gives practical guidance on keeping PCD safe and on legal disclosure.

### 16 Monitoring Compliance

| Compliance /effectiveness | Monitoring | Method | Freq. | Monitoring responsibility | Individual responsibility |
|---|---|---|---|---|---|
| Keeping PCD confidential | Local | Audit | BI-annually | IGoV Group : Toolkit | Staff / HoD |
| | Corporate | Audit | Annually | Corporate Governance Committee | HoD |
| Reporting PCD incidents | Sentinel | Analysis / trends interpretation | Quarterly | Corporate Governance Committee | PV |
| Caldicott Log disclosures/ | Log and reporting | Quality & Audit Lead | Quarterly | IG Committee | Q & A Lead |
| IG training figures | Monitoring Information | Security Coordinator | Quarterly | Clinical & Corporate Governance Committees | Education Lead (clinical) HR Director (non-clinical) |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |

## 17 Legislation

- Data Protection Act 1998.
- Human Rights Act 1998 and European Convention on Human Rights..
- Common Law Duty of Confidentiality.
- Freedom of Information Act 2000.
- Police and Criminal Evidence (PACE) Act 1984
- Road Traffic Act 1998

National Guidance

- ISO/IEC 17799:2005 (Information Security Standards).
- NHS Confidentiality Code of Practice 2003
- NHS Records Management Code of Practice 2006
- NHS Act 2006 and the NHS Constitution
- NHS Care Record Guarantee
- Caldicott Committee Report on the review of patient identifiable information 1997
- Caldicott 2 Review 2013, Information to Share and not to Share

**Associated Documents.** This policy should be read in conjunction with the following documents

- WSBH Information Security Policy
- WSBH Incident Management Policy
- WSBH Clinical Records Management Policy
- WSBH Consent to Treatment or Examination Policy
- WSBH Complaints Management Policy
- WSBH Information Governance Workdbook
- WSBH Employment Data Protection Policy HR19 V 3 (2015)

## Appendix 1 Eight Data Protection Act (1998) Principles

**1. Processed fairly and lawfully**

This is the most important principle. To comply, processing must be justified under one of several conditions set out in the Act. The most important condition is that the person has given his / her consent. Where the data is “sensitive”, consent must be “explicit”. Also, under this principle, a person must be fully aware of the ways in which their personal data may be processed in order for that processing to be considered fair.

**2. Processed for limited purposes**

Data may only be used for the purposes for which it was collected and not for other purposes.

**3. Adequate, relevant and not excessive**

Only information needed should be collected e.g. job applicants should not be asked to provide information whichwill only be needed for the successful candidate.

**4. Accurate and up to date**

Reasonable steps need to be taken to ensure the accuracy of information. This could include periodically checking that data held remains accurate and up-to-date.

**5. Not kept for longer than is necessary**
Personal data should not be kept for longer than is necessary. Equally, it should not be discarded if doing so would render the record inadequate. Specific legal provisions may require the retention of records for a set period (e.g. tax/compliance records). It may be necessary in some cases to retain information to defend legal claims which may be made in the future. Unless there is some legitimate reason for keeping them, personal data should be deleted.

**6 Processed in line with individuals' rights**
Individuals have a right to see information that is held about them. This is known as the right of "subject access". A subject access request must be dealt with promptly within 40 days of the date of receiving it. Not all information should be disclosed e.g. information about other people or which was received in confidence should not be disclosed.

**7 Data security** This principle requires that appropriate policies are in place to safeguard personal data including a data security policy; restricting access to data to authorized personnel; making sure that data is physically secure; training and educating staff about security measures; ensuring IT systems can withstand unauthorized access.
It also means ensuring that a contract is in place with any service provider appointed to carry out any data processing services, which includes clauses giving appropriate guarantees regarding data security.

**8 Not transferred to countries outside the EEA without adequate protection**
Transferring personal data outside the EEA without taking adequate legal precautions is a serious breach as it effectively means that data subjects lose the protection of the Act. There are a range of options as to how to carry out international data transfers legally.

The Data Protection Act 1998 defines regulation for the handling of personal data. The Act sets out that information must only be disclosed on a need to know basis. Staff need to safeguard the balance between the perceived need for information and the individual's right to respect for their privacy.
The following checklist has been compiled by the ICO to help comply with the Act:

- Do I really need this information about the individual?
- Do I know what I am going to use it for?
- Do the people I hold information about know that I hold it, and are they likely to understand what it will be used for?
- If I am asked to pass on personal information, would the people about whom the information is about expect me to do this?
- Am I satisfied the information is being securely held, either on paper or computer?
- Is our website secure?
- Is access to personal information limited to those with a strict need to know basis?
- Am I sure the personal data is accurate and up to date?

Do I delete or destroy personal information as soon as I have no more need for it?

## Appendix 2. WSBH Code of Confidentiality

**What is confidential patient information?**
1. A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

– It is a legal obligation that is derived from case law;

- It is a requirement established within professional codes of conduct; and
- It must be included specifically within employment contracts linked to disciplinary procedures.

2. Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this WSBH, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the WSBH of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. What this entails is described in more detail in subsequent sections of this document, but a key guiding principle is that a patient's health records are made by the health service to support that patient's healthcare.

3. One consequence of this is that information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

**Disclosing and using confidential patient information**

1. It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies. Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule, described later in this document, but it applies in most circumstances.

2. Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways.

**Patient consent to disclosing**

1. Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right.

Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it may mean that the is compromised. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment.

2. Where patients have been informed of the use and disclosure of their information associated with their healthcare; and that these choices may have implications then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent.

3. Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

4. There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Applications, and approvals, made under section 251 of the NHS Act 2006 (formerly section 60 of the Health and Social Care Act 2001) may support a range of important work such as clinical audit, record validation and research. Approved applications can be used to support disclosure without the consent of patients.

**Obligations on individuals working in the NHS**

1. All staff should meet the standards outlined in this document, as well as their terms of employment (or other engagement agreements). Much of what is required builds on existing best practice. What is needed is to make this explicit and to ensure that everyone strives to meet these standards and improves practice.
2. Clearly staff are constrained from meeting these standards where appropriate organisational systems and processes are not yet in place. In these circumstances the test must be whether they are working within the spirit of this code of practice and are making every reasonable effort to comply.

## Appendix 3 General Data Protection Principles (GDPR )2018

The GDPR principles are similar to those included in DPA, (1988) with additional detail and a new accountability requirement. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity.

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and current; all reasonable steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## Appendix 4 Caldicott Principles (Reviewed 2013)

The term Caldicott is derived from the 1997 Caldicott Committee report, which led to the publication of Confidentiality: NHS Code of Practice. This mandated that each organisation must have a Caldicott Guardian, to serve as the "conscience" of the organisation in relation to decisions about disclosure and ensure senior management of confidentiality matters.
WSBH is required to maintain and update their Caldicott Guardian registration managed by the Health and Social Care Information Centre (HSCIC). The Caldicott Guardian requires the cooperation of all staff in supporting fair, lawful and justifiable decisions to safeguard against harm to individuals or the WSBH's reputation.
The Caldicott principles (updated in April 2013) provide a guide for the use and transfer of PCD.
The seven Caldicott principles are the baseline for good practice;
Principle 1 – Justify the purpose(s) for using confidential information.
Principle 2 – Only use it when absolutely necessary.
Principle 3 – Use the minimum that is required.
Principle 4 – Access should be on a strict need to know basis.
Principle 5 – Everyone must understand their responsibilities.
Principle 6 – Understand and comply with the law.
Principle 7 – Duty to share information can be as important as the duty to protect patient confidentiality.
Individuals who believe that they have suffered damage as a result of misuse of their personal data may make a claim for compensation against WSBH and any negligent employee.
Additionally the ICO can fine the WSBH up to £500,000 as a penalty for serious breaches of the Data Protection Act.

## Appendix 5 NHS Care Record Guarantee and NHS Constitution

The NHS Constitution and NHS Care Record Guarantee set out the commitment to standards of confidentiality that patients/public can expect from NHS organisations and those providing care for NHS patients.

- Ensure, through contract terms and staff training, that all staff understand their duty of confidentiality, what it means in practice and how it applies to all parts of their work.
- Appropriate processes are in place to ensure all records are held securely and only made available to those who have rights of access.
- WSBH will take action when someone has deliberately accessed records without permission or good reason. This can include disciplinary action, ending a contract, firing an employee or bringing criminal charges. The person/s affected will be notified (Being Open).

## Appendix 6 Definitions:

**Accountable Officer / Chief Executive:** responsible for safeguarding charity / public funds/assets, ensuring value for money and sound financial and risk management systems.

**Anonymised Information**: Anonymisation requires the removal of name, address, postcode and any other detail or combination of details that might support identification.

**Caldicott Guardian**: is the confidentiality "conscience" of the organisation and ensures senior level oversight of the Information Governance agenda.

**Data controllers**: either alone or jointly determine the purposes for which and the manner in which any personal data are processed.

**Data Flow**: An exercise to review and record where data is sent, what data has been sent and the purpose of sending that data.

**Disclosure:** divulging or provision of access to data.

**Healthcare Purposes**: include all activities that directly contribute to diagnosis, care and treatment and the audit/assurance of the quality of healthcare provided. They do not include research, teaching, financial audit and other management activities.

**Health and Social Care Information Centre (HSCIC**): a national data, information and technology resource for health and social care driving care, services and outcome improvements; the source of authoritative healthcare data and information.

**Information Assets**: A collection of WSBH information (database, case-notes).

**Information Asset Register (IAR):** A list of information assets, administrators, owners and risk assessments used to understand and manage the asset risks.

**Information Asset Administrators (IAA**): managers responsible for maintaining the integrity of one or more information assets, managing information risks locally and keeping an information asset register. The IAA is accountable to the IAO and the IAO to the SIRO in relation to maintaining asset confidentiality and security (DPA compliance).

**Information Asset Owner**: manages information assets (within their remit) to comply with statutory obligations (Freedom of Information, Public Records Act and the Data Protection Act) and implement mandatory minimum standards for personal data handling.

**ICO:** Information Commissioner's Office.

Information Sharing Agreements (ISA): Documented rules and procedures for the sharing, disclosure and use of patient information in relation to security, confidentiality, and data destruction between two or more organisations or agencies.

**GDPR –** General Data Protection Regulation (2018)

**Personnel:** All WSBH staff and volunteers engaged in WSBH activities with access to personal, sensitive confidential information.

**Personal data** means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data

controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

**Privacy Impact Assessment (PIA):** Tool to identify and reduce new projects' privacy risks (See WSBH IGoV Policy).

**PCD:** Personal Confidential Information.

**Personal Confidential Data:** This is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people.

The review interpreted 'personal' as including the Data Protection Act definition of personal data, but included data relating to the deceased as well as living people, and 'confidential' includes both information 'given

**Processing:** obtaining, recording or holding information or data.

**Pseudonymised Information:** anonymised information cannot identify an individual. The original provider of the information may , however, retain a means of identifying individuals by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way true anonymisation does not.

**Safe Haven:** term used to explain either a secure physical location or the agreed set of administrative arrangements in place to ensure confidential personal information entering or leaving the organisation (fax, post or other means) is transmitted safely and securely. Any members of staff handling confidential information (paper or electronic,) must adhere to the safe haven principles.

**Sensitive personal information (or data)** means personal data consisting of information as to the racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, **and** the commission or alleged commission of any offence.

**Statement of Internal Control (SIC):** Public accountability document that describes organisational effectiveness of internal controls signed by the Accountable Officer.

**SIRO Senior Information Risk Owner** is the WSBH's Chief Operating Officer leads the Information Governance culture, owns the WSBH IGV management incident and risk management framework and advises the AO (Data Protection & Confidentiality. EPR: Electronic Patient Record

See the Trust's Information Governance Assurance Framework Strategy.

| **Short Form Equality Impact Assessment** | | | |
|---|---|---|---|
| 1. | Briefly outline of the key objectives of the policy; what it's intended outcome is and who the intended beneficiaries are expected to be | *To provide clear guidance for the management of approved procedural documents* | |
| 2. | Does the policy have an impact on patients, carers or staff, or the wider community that we have links with? **Please give details** | *Yes facilitates detail organisational functions and responsibilities and assure compliance with national standards, best practice guidance and organisational strategy and goals.* | |
| 3. | Is there any evidence that the policy \ service relates to an area with known inequalities? **Please give details** | *None* | |
| 4. | Will/Does the implementation of the policy \ service result in different impacts for protected characteristics? | | |
| | Disability | Yes | *No* |
| | Sexual Orientation | Yes | *No* |
| | Sex | Yes | *No* |
| | Gender Reassignment | Yes | *No* |
| | Race | Yes | *No* |
| | Marriage/Civil Partnership | Yes | *No* |
| | Maternity/Pregnancy | Yes | *No* |
| | Age | Yes | *No* |
| | Religion or Belief | Yes | *No* |
| *If you answer 'Yes' it may be necessary to carry out a full Equality Analysis. Refer to ratifying committee.* | | | |
| The above named policy has been considered and does not require a full equality analysis | | **Date: 17.01.2018** | |

| | |
|---|---|
| **Corporate Governance Committee** | |