Policy & Procedure: Information Governance

Introduction
Information governance is a wide reaching, fundamentally important issue for our service provision. This policy and procedure is designed to inform, and where necessary instruct staff and volunteers on how to perform their duties and responsibilities in line with both the law and the organisation's standards of good governance.

Service users at Blythe House 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 a legitimate expectation that staff and volunteers will respect their privacy and act appropriately.

The 25th May 2018, General Data Protection Regulations (GDPR) officially came into effect. The GDPR will build on the 1998 Data Protection Act but strengthens and standardises data protection across the EU.

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

These principles form the basis of how Blythe House processes personal data

The GDPR also creates some new rights for individuals and strengthens some of the rights which currently exist under the Data Protection Act

- **The right to be informed.**
    - Encompasses a company's obligation to provide "fair processing information", typically through a privacy notice. The information a company supplies to an individual depends on whether that personal data was obtained directly or indirectly. Information about the processing of personal data should be provided free of charge and be concise, transparent and easily accessible.

- **The right of access.**
    - An individual has the right to obtain; confirmation that their data is being processed, access to their personal data; and other supplementary data. Companies must provide a copy of the information free of charge. They may only charge a "reasonable fee" where the request is manifestly unfounded, excessive or repetitive. The information must be provided without delay and within one month of the request,

- **The right to rectification.**
    - Individuals are entitled to have personal data rectified it is inaccurate or incomplete. Companies must respond within one month unless the request is complex, and if you have disclosed the personal data in question to third parties you must also inform them of the rectification where possible.
- **The right to erasure.**
    - Also known as “the right to be forgotten”. Individuals have a right to have personal data erased and to prevent processing in certain circumstances. For example, to comply with a legal obligation
- **The right to restrict processing.**
    - Similar to the DPA, individuals can block or suppress processing of their personal data. In these cases, companies can store the personal data, but not process it.
- **The right to data portability.**
    - This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.
- **The right to object.**
    - Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority; direct marketing; and processing for the purposes or scientific or historical research and statistics.
- **Rights in relation to automated decision making.**
    - The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to those under the DPA.

The medical profession, and therefore Blythe House Hospice, has always had a duty to keep information confidential. This duty goes back to the Hippocratic Oath in Ancient Greek times, therefore it is not new, it is a legal requirement and everyone must comply. As an organisation, Blythe House Hospice processes personal information for the purpose of providing healthcare.

Personal confidential data relates to a living individual who can be identified. Breaches in data protection will seriously damage the reputation of Blythe House and adversely affect donations and community support.

- Personal confidential information is made up of personal identifiers, which used alone or in combination can identify an individual. They were listed by the Data Protection Act 1998 as:

Forename	ID number
Surname	Ethnic origin
House number and street	Gender
Postcode	NI number
Date of Birth	Credit
NHS number	Bank account

The GDPR 2018 specifies that any personal data relating to the following subject matter will now be under special categories of personal data, such as:

  - the racial or ethnic origin of the data subject.
  - their political opinions
  - their religious or philosophical beliefs
  - whether they are a member of a trade union
  - their physical or mental health.
  - their sexual life or sexual orientation
  - their genetic or biometric data (e.g. fingerprints/facial/iris recognition systems).

- Data protection applies whenever a data controller within the organisation, which for Blythe House is the CEO, processes personal data. We do this every day at Blythe House with the personal data of our service users.

Confidentiality

Confidentiality is an obligation for all staff, volunteers and external contractors.

Breach of confidentiality, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings.

- The duty of confidentiality arises out of the common law of confidentiality, professional obligations, and staff employment contracts.
- All members of staff must ensure that they are aware of the requirements and standards of behaviour that apply. Volunteers and students are also under obligations of confidentiality and will be required to sign an agreement indicating their understanding of this when supporting our services.
- It is vital that there is no gossiping, this is clearly an improper use of confidential information.

- Do not discuss patient cases in public places.
- It may be pertinent to discuss cases with colleagues for professional reasons e.g. to gain advice or share experience and knowledge, but every effort must be made to ensure that others do not overhear these conversations. Generally, there is no need to identify the service user concerned.
- Service users have different needs and values and this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information.
- Service users have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care. The disclosure of information for healthcare purposes is not normally an issue for the great majority of service users.

- There are four main requirements in providing a confidential service:
    - **Explain:** Explain the implications of disclosing and not disclosing. In order to make valid choices, service users must not only know what their options are, but also what the consequences are of making those choices. Where service users insist on restricting how information may be used or shared in ways that compromise the health service's ability to provide them with high quality care, this should be documented within the service user's record. It should be made clear to the service user that they are able to change their mind at a later point.
    - **Ask:** Ask service users for their permission before using their personal information in ways that do not directly contribute to or support the delivery of their care e.g. research.
    - **Respect:** Respect service users' decisions to restrict the disclosure and/or use of information. In some cases it may not be possible to restrict information disclosure without compromising care. This requires careful discussion with the service user, but ultimately the service user's choice must be respected.
    - **Continuous Improvement:** It is not possible to achieve best practice overnight but in

All staff must be aware of the basic requirements and where support and further information are available. If you need training and guidance to develop confidential practices seek it out.

- All staff must work within the framework of this policy and be able to demonstrate that they are making every reasonable effort to comply with relevant standards.
- Essential points to remember include:
    - **Make clear to service users when information is recorded or health records are accessed:** this may require no more than a comment such as *'Let me note that in your file'* or *'I am just taking a note of your blood pressure'*, and should occur naturally as a part of treating service users properly.
    - **Make clear to service users when information is, or may be, disclosed to others:** service users may know little about how the organisation and related agencies e.g.

hospitals, social services, local government and education work, aspects that staff may take for granted.

- **Ensure that patients know when data is disclosed or used more widely:** there are certain Acts of Parliament that require disclosure and court orders may also require a disclosure. The amount of information disclosed should always be proportionate to the actual need. Even though the service user cannot prevent this disclosure, they must normally be told that it is taking place or that it has already occurred if this is the case. Service users must be made aware that the information they give may be recorded, shared in order to provide them with care, or used to support local clinical audit and other work to monitor the quality of care provided.

- **Respect the right of service users to have access to their health records:** service users have a right to see and/or have copies of their health records under the Data Protection Act.

- **Communicate effectively with service users to help them understand:** it is important to recognise the different communication needs of service users.
  - **Difficulty in communicating does not remove the obligation to help people understand:** care must be taken to ensure that information is provided in a suitable format or language that is accessible.

  - **Communicate effectively with service users to help them understand:** if a service user has difficulty communicating their wishes it is important to check for a clear and unambiguous signal of what is desired by the service user and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Equality Act 2010, would contravene the Accessible Information standard and may prevent consent being gained.

Caldicott Principles

- **Principle 1: Justify the purpose(s) for using confidential information**
  Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised 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 items 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 is 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 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 every organisation that handles 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 the policies of their employers, regulators and professional bodies.

- Th **Remember the Caldicott principles and you won't go wrong.** nt ones is...'A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian who is responsible for safeguarding the confidentiality of patient information'.

The Caldicott Guardian for Blythe House is the CEO

- The Caldicott Principles also cover technical measures and procedures which need to be in place and are basically common sense.

- This can include:
  - Allocation of individual access levels
  - Password controls: setting up individual user ID and passwords to access computer held databases
  - Screen savers
  - Privacy screens: computer terminals sited so that patient information and other confidential information on screen cannot be seen by unauthorised people. Unauthorised viewing of personal information is a breach of confidentiality
  - Virus detection software to protect from computer viruses
  - Prohibiting the use of unauthorised software on the organisation's system thus avoiding the possibility of viruses
  - Audit trails/reports
  - Guidelines for users
  - Back-ups: making regular copies of computer held data
  - Use of networks /e-mail /Intranet.

Information Security

- Information, whether in paper or electronic form, is the lifeblood of the hospice because of its critical importance to service user care and other business processes.

- It has greatest value when it is accurate, up to date and is accessible where and when it is needed.

- Effective information security management ensures that information is properly protected, secure, confidential and reliably available.

- Much of the information used at Blythe House is held in IT systems. Some of this data is subject to legal and regulatory obligations as well as being important for operational reasons. In order to comply with these obligations, electronic information should be held securely to protect confidentiality, prevent loss or damage and have the right information available at the right time to the right people.

- The CEO has overall legal responsibility for complying with legal requirements. However, keeping information secure is the responsibility of all staff and volunteers who must ensure that breaches of confidentiality do not occur as a result of their actions. Information in the wrong hands can be devastating and if individuals facilitate this in any way they could be liable for prosecution.

People and the precautions they take are the key to good security!

Information Security

There are three main elements of information security.

- **Confidentiality:** protection against unauthorised access or disclosure
- **Integrity:** the integrity and evidential value of information should be maintained
- **Availability:** information should be available to properly authorised staff as and when it is required.

If computers are to be left unattended they should be made secure so that information cannot be accessed by unauthorised persons, this can be done by logging out or locking the computer.

Securing the Work Area

It is important to consider how security can be breached in the work area:

- All lockable filing cabinets should be locked
- All confidential paperwork should be locked away
- Portable IT equipment should be locked away in a lockable cupboard or filing cabinet.
- Windows and doors should be closed
- If there is an alarm this should be set
- If doors are password protected ensure that the lock is engaged.

Passwords are essential to:

- allow users to gain access to their own personal information or services electronically
- allow users to gain access to other's personal information if required to do their job
- prevent unauthorised access to computer systems, online services, email accounts, electronic files or restricted premises
- keep information secure and confidential.

Appropriate Use of Portable I.T. Equipment and Media

- Portable IT equipment can be a laptop, mobile phone or blackberry
- Points to remember when using a laptop from Blythe House
  - when not in use, store in a secure location, ideally a locked cabinet in a locked office
  - never leave portable equipment on view in a car or any public area
  - where possible, use a locking cable to tether a laptop when in use
  - use the secure remote access services where relevant
  - all laptops must have approved anti-virus software installed.

Personal Identifiable Data (PID)

If data is stored on the local hard drive, usually C: Drive, of a laptop and it is lost or stolen, then so is the data.

If this is personal data the loss is a breach of the Data Protection Act and confidentiality.

If personal identifiable data is sent via email externally e.g. to another organisation this is not 100% secure unless the information is encrypted first.

Portable / Removable Media: USB; CD; secure digital card; DVD; external hard drive; cloud storage

- It is the organisation's responsibility to ensure mobile data and devices, and in particular data that contains 'personal identifiable data', is kept secure. All members of staff must ensure the following when using portable media and personal identifiable data.

Under no circumstances should personal data be transferred to a USB or CD and removed from Blythe House.

Appropriate Use of Email

- Junk email and chain letters sent via email are known as spam. Do not keep or forward them to other users. **Delete them.**
- **Never** reply to junk email even if there is a link to an unsubscribe facility. If you do reply, it confirms that yours is a valid email address and will result in you receiving more junk email.
- All members of staff are expected to manage their email facility in a professional manner and to remember that it is primarily provided for work purposes.

Use of Internet

- This is for business purposes and **limited** personal use.
- Inappropriate use of the internet at work is a serious disciplinary offence.

Unauthorised Software

- Unauthorised software must not be used and potential viruses or unusual activity on the computer must be reported immediately.

Information Sharing

- Everyone deserves high quality and effective care services to be delivered to them by the right person at the right time. To ensure the successful delivery of services, organisations such as Blythe House recognise that they must work together to provide seamless care.

- In order to co-ordinate such services, avoid duplication and ensure the most suitable services are provided, where appropriate and relevant, information must be shared between organisations to provide effective care.

Sharing for care provision

We can share information if it relates to the continued care and/or treatment of a service user. An agreement is not required as long as there are adequate security and confidentiality procedures in place.

When to Share?

- It can often be difficult for staff to decide whether or not to share service user information and reluctance often comes from fear of breaching GDPR 2018. In some circumstances lack of information sharing could compromise care.

Care Provision

- As an organisation, Blythe House has to show that we have a strong information governance framework and that all staff are aware of their responsibilities regarding the Caldicott Principles, confidentiality, data protection and information security.

Legal Disclosures of Information

- There is some legislation which places a strict requirement on the organisation to disclose information. However, care should be taken to only disclose the information required to comply with and fulfil the purpose of the law. If staff have a reason to believe that disclosure would cause serious harm to the service user or another person, legal advice should be sought.

- The courts, including the coroner's courts, have legal powers to require that information may be disclosed within their jurisdiction. This does not require the consent of the service user whose records are to be disclosed but they should be informed, preferably prior to disclosure.

Disclosures in the Public Interest

- Under common law, members of staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge that the public good achieved outweighs the obligation of confidentiality to the individual patient concerned.

- There must be a record made of the disclosure so there is clear evidence of the reasoning used and the circumstances as to why this was done. Wherever possible, the issue of disclosure should be discussed with the individual concerned and consent sought and for them to be told of any decision to disclose against their wishes. This is not possible in all cases e.g. where likelihood of a violent response is significant.

Data Quality

- Data quality refers to the quality of data we hold within the organisation either in paper or electronic format.

- Data is of high quality *"if it is fit for its intended use in operations, decision making and planning".*

- High quality information is:
  - accurate
  - up to date
  - quick and easy to find
  - free from duplication e.g. where two or more records exist for the same service user.

- High quality data is vital for Blythe House because we need:
  - accurate and timely information to manage services and accountability
  - good information to manage service effectiveness
  - to prioritise and ensure the best use of resources
  - to report to auditors and inspectors who will make judgements about our performance and governance.

- Blythe House holds data on service users, staff, donors and volunteers.

- Clinical staff need to be able to rely on the accuracy of information available in order to be able to provide timely and effective treatment for a service user.

Improving Data Quality

Staff can help to improve data quality by

- ensuring that they check service users' demographic details at every appointment
- including the service user's NHS number on all communications within the organisation and to service users themselves
- getting information right first time; this reduces the problems in the long term
- checking that a person is not already on the system before adding them as a new registration, in order to avoid duplicate records.

The Benefits of High Quality Data

- Service users will receive better, safer care from the organisation if the quality of information held about them is accurate, up-to-date and readily available.

- Staff have greater levels of confidence that they are advising service users about the best care for them on the basis of accurate, up to date, complete information.

- Staff and volunteers feel secure in the knowledge that their information is accurate in terms of human resources and this will ensure that their future training and work within the organisation is based on that.

Records

Record keeping

Blythe House may need to keep health records in various formats:

- Computerised records
- Correspondence between health professionals
- Laboratory reports
- X-ray films and other imaging records
- Photographs
- Handwritten notes made by a healthcare professional or support staff.

Health records

The characteristics of full and accurate health records are:

- Authentic
- Reliable
- Complete and unaltered
- Processes and systems which have integrity
- Useable
- Transferrable
- Structured.

We keep health records for:

- Continuity and evaluation of patient care
- Risk management
- Clinical governance
- Resource utilisation
- Research and education
- Effective communication between members of the health care team
- As a historical record of events which can be referred to if required in the future e.g. during legal inquiries, internal investigations or for future health care purposes
- To fulfil professional requirements e.g. GMC; NMC; Fundraising code of conduct.

Records Management

A health record should be available in the right place at the right time to support effective service user/carer contact and to provide continuity of care.

- Each notation must be accompanied by the full date and time, using the 24-hour clock, plus the signature and printed name of the person making the entry to ensure that each entry can be attributed to an individual
- Notations must be factual, consistent, accurate and chronological
- Notations should be written as soon as possible after an event occurs, providing current information on the care and condition of the service user
- If the notation is handwritten it must be written clearly using black indelible ink

Continued over…

- The notation should be free from jargon, irrelevant speculation or subjective statements and only approved abbreviations can be used
- The notation must be compliant with use of approved patient identifiers e.g. full name of service user
- Incorrect entries should be crossed out with a single line and edited within the electronic care record to ensure correctness
- Any justifiable alterations or additions must be dated, timed and signed, and clearly attributable to a named identifiable person and the original entry still able be read clearly
- A written provisional diagnosis and reason for referral must be recorded
- Notations should enable the multi-disciplinary team to communicate effectively.

- All clinical records will maintain confidentiality of the information to be documented or recorded
- Care must to be taken to ensure that service user information cannot be viewed on computer screens by those who have no right to view
- Paper reports/letters should be scanned and attached to the electronic clinical record and the original documents shredded
- Members of staff must comply with requirements of the GDPR 2018 at all times.

Members of staff are responsible, by law, for any record they create or use and have a common law duty of confidentiality to service users. This continues after the death of a service user and after the member of staff has left the organisation.

Always remember that a well-maintained health record will reflect well on the organisation.

Safe Haven

- A Safe Haven is a 100% confidential environment. All organisations should have a Safe Haven and use it according to a set of guidelines. A Safe Haven safeguards patient information flowing to and from the organisation.

- Ideally all information exchanged between organisations will pass between safe haven points.

- When information is disclosed by a designated safe haven point to an equivalent point in another organisation, staff can be confident that information is being transported securely and confidentially.

- To create a 100% confidential environment the following must be considered:
  - Internal and external post
  - Telephones including answer phones
  - Fax machines
  - Electronic information/email
  - Information storage
  - Whiteboards.

- It is the responsibility of every member of staff to ensure that each of the above are managed to ensure that the security and confidentiality of patient information is maintained at all times.

Telephone

- Information should be passed over the telephone as part of an agreed process with the service users concerned and where the need and authority to share information has already been set up.

What information can be given to relatives/next of kin?

- Check the caller's identity and the full name of the service user to whom the enquiry is related
- Consider the information you are giving out: clinical details must **not** be given out without the consent of the service user, who may not want this information to be passed on to others including relatives
- Consent must be gained from service users with regard to who they will allow staff to discuss their health matters with. If this is not possible owing to the service user's condition, members of staff will be required to make their own judgment in the service user's best interest. If in doubt take the caller's contact number and phone them back.

- If you remain unsure of the caller's identity and how to proceed, talk to your manager.

What information can you give to other staff?

- Check the identity of the staff member, their name, department and nature of the enquiry
- Request their telephone number and call them back
- If there is need for clinical information to be released, be aware of who may be listening.

Information that can be given to the Police

As an organisation we are obliged to disclose information if it relates to a serious crime, rape, murder or treason. For any other information requests, a letter signed by the Superintendent must be sent to the organisation via mail or fax before we can respond to the request and the required consent procedures.

Information that can be given to the Media/Press

All media contact must be passed to the CEO or the Fundraising & Communications manager or, in their absence, refer to the senior manager on duty. Under no circumstances should any personal information be given out without permission.

Answer Phones/Voice Mail

- When required to contact a service user by telephone, you must gain consent from them in advance to establish that they are happy for you to leave a message, if necessary. This consent and any other requirements must be recorded in their health record.

- If you are required to leave a message on a service user's answer phone/voice mail without prior consent do not leave any details regarding the organisation or any clinical information. The only information that may be left is your name, telephone number and a brief message asking them to call you back.

- Members of staff must not leave messages for service users if there is any doubt regarding the validity of the telephone number or it is not possible to be sure that:
  - other people won't hear the message
  - the correct telephone number was used
  - the recipient can fully understand the message
  - confidentiality isn't breached by informing someone, who was previously unaware, that the person is using Blythe House services.

Using the Telephone: Do's and Don'ts

- We all have a duty of confidentiality. When discussing a service user's care or staff issues remember that conversations can be overheard. If you don't need to identify service users or staff by name then don't.

- If you are discussing a service user or member of staff ensure that this is carried out in an area where you cannot be overheard e.g. in a locked office away from a public or staff area.

- Conversations about service users on public transport or in any public place can be overheard by other people and is not acceptable. This is a breach of confidentiality.

Using the Fax Machine

- It is not recommended to routinely send personal and clinical details via fax. Faxing service user information is only justifiable in situations where not doing so could impact on the health of the service user.

- When faxing personal/confidential and/or sensitive information, you must advise the recipient that you are sending the fax, so they know it is coming and can be ready to receive, and vice versa.

- Always confirm with the sender that you have received a confidential fax.

- It is good practice to send double fax transmissions, one containing the service user's details, which is anonymised as much as possible and the other containing the clinical details with a linking identifier to link the faxes together.

- Use the fax header as follows:

  "Fax Disclaimer: The content of this transmission is intended for the named addressee only. It contains information, which is confidential and legally privileged. Unless you are the named addressee, or authorised to receive this transmission for the addressee, you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please contact "your

name" on the following telephone number, and then confidentially destroy any copies of it"

- Always confirm the fax has been received by the right person.
- Request a report sheet to confirm safe and correct transmission.

Sending Personal Information by Post

- The information should be placed inside an envelope and be clearly marked with the recipient's name and address.
- The front of the envelope should be marked **"Private and Confidential"**.
- Ensure the seal is tamper proof by placing Sellotape or sticky tape over the seal rather than using the seal to close the envelope. Self-seals can come unstuck and loss of data can occur.
- It is good practice to record what items of post have been sent and on what date, so that they can be tracked in case of loss or queries.

Disposal of Confidential Information

Confidential paper waste should be disposed of in the following ways:

- By using a shredder
- By using a confidential waste console where paper can be posted in a secure unit, which is collected on a regular basis and the contents shredded securely.

Never put paper containing personal identifiable information into general waste bins

Supporting legislation:

- GDPR 2018
- Data Protection Act 1998
- Caldicott Principles revised 2013
- Freedom of Information Act 2000
- Safe Haven Guidance North Derbyshire CCG 2015

- Access to Health Records Act 1990