CONFIDENTIALITY AND DISCLOSURE OF INFORMATION INCLUDING:

- ☑ *Human Rights Act 1998*
- ☑ *Data Protection Legislation / GDPR*
- ☑ *Freedom of Information Act 2000*
- ☑ *Access to Health Records Act 1990*
- ☑ *Computer Misuse Act 1990*
- ☑ *Health and Social Care Act 2014*
- ☑ *Common Law Duty of Confidence*
- ☑ *Use of smart phones*

VERSION No	**4**
REVIEWED BY	**Mariana Philipova**
NUMBER OF PAGES	**19**

POLICY STATEMENT

It is the policy of this home that:

- ☑ ***we will protect information on the basis of:***
  - ➢ ***confidentiality*** *(ensuring that information is accessible only to authorised individuals)*
  - ➢ ***integrity*** *(safeguarding the accuracy and completeness of information)*
  - ➢ ***availability*** *(ensuring that authorised users have access to relevant information when required; 'on need to know basis')*
  - ➢ ***relevance*** *(only keeping what we need for as long as it is needed)*
- ☑ ***we will meet all regulatory and legislative information management requirements***
- ☑ ***we will maintain business continuity plans (in cases of accidents, 'acts of god', etc.)***
- ☑ ***we will deliver appropriate information security training to all staff***
- ☑ ***we will make available appropriate and secure tools to all staff***
- ☑ ***we will report and follow-up all breaches of information security, actual or suspected***

LEGAL BASIS

The home must comply with all relevant UK and European Union legislation, including:

- ☑ *Human Rights Act 1998*
- ☑ *Freedom of Information Act2000*
- ☑ *Data Protection Legislation / GDPR*
- ☑ *Access to Health Records Act 1990*
- ☑ *Computer Misuse Act 1990*
- ☑ *Health and Social Care Act 2014*
- ☑ *Common Law Duty of Confidence*

SCOPE AND APPLICATION

This policy applies to all staff members, whether permanent, temporary or contracted in (either as an individual or through a third party supplier such as agency).

- ☑ Information sharing is a vital component in any employer-employee relationship and is a vital component of the service we provide to our service users. The company aims to promote openness and transparency, both within our organisation, and to our service users and their families. It is important to recognise the need to disclose information legitimately and to ensure the data transfer is done securely.

- ☑ It is a criminal offence under the Data Protection Legislation knowingly or recklessly, without the consent of the organisation, to obtain or disclose personal data or the information contained in personal data, or obtain the disclosure to another person of the information contained in personal data.

- ☑ In the course of their employment with our company, staff members have the authority to obtain and disclose personal data, but they will commit a criminal offence if they use this position to obtain, disclose, or obtain disclosure of personal data for their own purposes.

- ☑ Discrimination means treating people differently without an objective or reasonable justification for the difference in treatment. All staff members are expected to treat information provided in confidence by individuals confidentially; irrespective of their race, disability, gender, age, sexual orientation, religion or belief, or socio-economic status. Discrimination by staff members is unacceptable behaviour and will not be tolerated by the home.

- ☑ Individuals have the right to object to the use and disclosure of confidential information which identifies them. Special attention should be paid to the issues around consent. The Data Protection Legislationrequires an organisation to obtain consent from an individual to process their personal data. The Act does not define what type of consent must be sought, and consent can be implied as long as the individual is informed. However, when processing sensitive personal data explicit consent should be sought.

- ☑ Information should be accessed by staff only 'on need to know basis'. Staff members are not permitted to gain access or attempt to gain access to information they do not need to see to carry out their work. This includes viewing the personal data (or sensitive personal data) of family members, colleagues, celebrities, friends or neighbours.

- ☑ The home Terms and Conditions of Employment stipulate the Confidentiality clause staff members are bound to comply with and are required to sign a confidentiality agreement prior to commencing employment.

- ☑ A number of staff members will also be duty-bound by the professional codes of conduct of their respective professions, which contain confidentiality principles such as Registered Nurses.

- ☑ Staff members are responsible for the data they disclose and this is a huge personal responsibility because of the legislation that governs the processing of data. If staff members are in any doubt as to whether they can legally disclose the information that has been requested from them, they should always seek advice from a senior member of staff.

- ☑ Staff members who breach the confidentiality of another person during the course of their employment, by recklessly disclosing the personal data or sensitive personal data relating to that person or another person who can be identified from that data may be disciplined using the Disciplinary Policy and Procedure This will ensure that all disciplinary matters are dealt with in a fair, reasonable and consistent manner.

DEFINITIONS AND EXPLANATION OF TERMS

This section provides staff members with an overview of the following definitions and explanation of terms:

- ☑ Information and data (personal, company, etc.)
- ☑ Concept of Confidentiality;
- ☑ The Caldicott Committee Principles.

1. Information and data

a) Information results from the acquisition and collation of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper) phone calls and conversations. For the purpose of this policy information and data can be regarded as the being the same.

b) **Sensitive and confidential information.** The following list is not exhaustive and contains examples of sensitive and confidential information:

- ➢ Person - identifiable information, e.g. service user and employee records; and may include: medical records, employment records, financial records, etc.
- ➢ Company records containing organisationally sensitive information
- ➢ Any commercially sensitive information such as information relating to commercial proposals or current negotiations

- Politically sensitive information
- Information relating to security, investigations and proceedings
- Information provided in confidence

An easy sense check on whether information is sensitive or confidential is:

- Is the information covered by the Data Protection Legislationor any further duty of confidence (refer to the Data Protection Principles later)?
- Could release of the information cause problems or damage to individuals, the public, the home or a partner organisation? This could be personal, financial, reputation or legal damage.

2. Concept of Confidentiality

- *When staff members apply to the home to gain employment, they provide the organisation with personal details about themselves in order to process their application. They give these details with the legitimate expectation that the home would process them in a confidential manner.*
- *When a caller telephones the home and provides their personal details or personal details of a third party person they are seeking our services for, they also have the expectation that we will process them in a confidential manner.*
- *A duty of confidentiality arises when a person discloses information to another person under conditions where it is realistic to expect that the information provided will be treated in confidence.*

3. Human Rights Act 1998

- This Act came into force on 2nd October 2000 and allowed the European Convention on Human Rights to become enforceable in the United Kingdom. The Act gives people a clear legal statement of their basic rights and fundamental freedoms. For the home this means that everything we do must be compatible with the Convention rights unless an Act of Parliament makes that impossible.
- The Convention right which relates to confidentiality is: ***Article 8: Right to Respect for Private and Family Life***
  - ☑ Everyone has the right to respect for his private and family life, his home and his correspondence.
  - ☑ There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- Article 8 is a Qualified right. These are rights which require a balance between the rights of the individual and the needs of the wider community or state interest. Qualified rights can be over-ridden when it is in the public interest or there is a clear legal basis to do so.

4. Data Protection Legislation

a) Need for the Data Protection is vital because there are:

- *Concerns about large amounts of personal data being held unnecessarily*
- *Concerns about people having access to this information*
- *Concerns about personal information getting lost or stolen if not adequately protected*
- *The Data Protection Legislation sets standards governing the storage and processing of personal data held in manual records and on computers*
- *It places a duty on those who keep personal records to be open about their use of the data and to follow the 8 data protection principles*
- *Applies to computerised and manual records*
- *Makes 'sensitive' data subject to special treatment*
- *Stresses the confidentiality of information*
- *States that data should be 'shared' only when necessary*
- *Gives individuals rights to access information about themselves. Individuals have a right to know what information organisations hold about them. They can submit an Access Request to see or have a copy of any information*

☞ *Organisations must identify an 'information controller'. In this home the 'Information Controller' is the Administrative Assistant.*

i. The table below contains the 8 Data Protection Principles:

PRINCIPLE 1	**Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:** a) At least one of the conditions in Schedule 2 (see Appendix A) is met, and b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 (see Appendix B) is also met.
PRINCIPLE 2	**Be held for specified and lawful purposes.** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
PRINCIPLE 3	**Personal data shall be adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.
PRINCIPLE 4	**Personal data shall be accurate and, where necessary, kept up to date.**
PRINCIPLE 5	Personal data processed for any purpose or purposes **shall not be kept for longer than is necessary for that purpose** or those purposes
PRINCIPLE 6	Personal data shall be processed in accordance with the rights of data subjects under the legislation.
PRINCIPLE 7	Appropriate technical and organisational **measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**
PRINCIPLE 8	Personal data **shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection** for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Common Law Duty of Confidentiality

This is the law which is laid down in decisions made by our Courts as opposed to being a written Act of Parliament. It is sometimes referred to as 'case / precedence law' where a Court will make a decision or ruling based on previous cases.

Past judgments have allowed confidentiality to be breached when there is a clear legal basis or over-riding public interest to do so. This is judged on a case-by-case basis. The general principle, however, is that information provided in confidence will remain so.

3. Freedom of Information Act 2000

The Freedom of Information Act 2000 came into force fully in January 2005 and deals with access to official information. It grants a right of access to information held by public authorities and is intended to improve democratic processes by giving the public greater access to information about the workings of Government. It gives individuals or organisations the right to request any recorded information held by a public authority. Information such as staff e-mails, minutes of meetings, research papers, reports etc can be requested. Certain information can be exempted from release.

The Freedom of Information Act 2000 provides access to information held by public authorities and is different to Data Protection legislation which is concerned with personal data held by all companies registered to hold such data.

a) Public Authorities: These include government departments, local authorities, unitary authorities, the NHS, state education sector, police forces etc. It does not however cover every organisation that receives public funding e.g., charities, or certain private sector organisations that perform public functions.

b) Definition of "Information": The Act covers any recorded information that is held by a Public Authority in England, Wales and Northern Ireland. Recorded information includes:

- Printed documents
- Computer files
- Letters
- Emails
- Photographs
- Sound or/and Video recordings.

The Act ensures information is available in two ways. Public authorities are obliged to publish certain information about their activities, and Members of the public are entitled to request information from public authorities.

c) Principles: "*Openness is fundamental to the political health of a modern state. The white paper marks a watershed in the relationship between the government and people of the United Kingdom. At last there is a government ready to trust the people with a legal right to information." "Unnecessary secrecy in Government leads to arrogance in governance and defective decision making*."

d) Your Right to Know 1997: The main principle behind Freedom of Information is that, quite simply, people have a right to know about the activities of public authorities, unless there is a good reason for them not to. This is sometimes described as a presumption or assumption in favour of disclosure. This means that:

- Everybody has a right to access official information Disclosure should be the default-in other words information should kept private only when there is a good reason and it is permitted by the Act.
- An applicant (requestor) does not need to give a reason for wanting the information on the contrary, public authorities must justify the refusal.
- They must treat all requests equally, except under some circumstances relating to vexatious requests and personal data.
- The information someone can obtain under the Act should not be affected by who they are. All requestors should be treated equally whether they are journalists, local residents, public authority employees, or foreign researchers and because they should treat all requestors equally, they should only disclose information under the Act if they would disclose it to anyone else who asked.
- In other words you should consider any information released under the Act as being released to the world at large.
- Schedule 1 of the Act contains a list of public bodies that are covered by the Act.
- Section 5 of the Act gives the Secretary of State the power to designate further bodies as public authorities.
- With effect from 1st September 2013 public authorities now include companies wholly owned:
  - By the Crown
  - By the wider public sector or
  - By both the Crown and the wider public sector.

e) Who can make a request?: Anyone can make a freedom of information request you do not have to be a U.K resident or a U.K citizen. They can be made by organisations e.g. newspaper, campaign group or company. Requestors should direct their request for information to the public authority they think will hold the information. When appropriate, this organisation will assist individuals to access freedom of information requests by signposting to sources of advice such as Citizens Advice Bureau etc.

4. The Caldicott Function

In December 1997 the Caldicott Committee chaired by Dame Fiona Caldicott issued a report on the 'Review of Service user-Identifiable Information'. This was commissioned by the Chief Medical Officer of England who asked the committee to review the transfer of service user-identifiable information from NHS organisations to other NHS and non - NHS organisations which is applicable to all staff in this home.

The committee made 16 recommendations and proposed 6 principles to be applied when processing service user-identifiable information. These 6 principles are known today as the Caldicott Principles.

In the table below are the general principles taken from that report:

PRINCIPLE 1	***Justify the purpose(s)***
	Every proposed use or transfer of service user-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
PRINCIPLE 2	***Do not use service user-identifiable information unless it is absolutely necessary***
	Service user-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for service users to be identified should be considered at each stage of satisfying the purpose(s).
PRINCIPLE 3	***Use the minimum necessary service user-identifiable information.***
	Where use of service user-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
PRINCIPLE 4	***Access to service user-identifiable information should be on a strict need-to know basis***
	Only those individuals who need access to service user-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes. For example: a different of pass word for an access of a company computer.
PRINCIPLE 5	***Everyone with access to service user-identifiable information should be aware of their responsibilities***
	Action should be taken to ensure that those handling service user-identifiable information: both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect service user confidentiality.
PRINCIPLE 6	***Understand and comply with the law***
	Every use of service user-identifiable information must be lawful. Someone in each organisation handling service user information should be responsible for ensuring that the organisation complies with legal requirements.

5. Equality Impact Assessment

It is the home's policy to that meet the diverse needs of our service users and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010 and data handling and processing.

6. How to ensure information remains Confidential

a) The home receives many requests to disclose information. These could be ***Subject Access Requests*** *(gives an individual the right under the Data Protection Legislation to find out if and what personal data the home has on an individual. On payment of a fee to the home, the individual will be provided with a copy of that data once reasonable checks have been made to establish the identity of the requestor and their rights to that information.)* for personal data made under Data Protection legislation or requests for company data made under Freedom of Information legislation. There are also other legal entities that have the right of access to our data, where we are obliged under another Act of Parliament to disclose this data without breaching the confidentiality or gaining

the consent of the individual concerned. We also have to disclose information if required to do so by a Court Order.

b) Only certain staff members have the authority, which is dictated by their role, to disclose confidential data.

c) A spurious request (false request) for data can occur when somebody impersonates another in order to obtain data fraudulently. Take care not to fall foul of a spurious request. Staff members should take reasonable steps to verify the identity of the requestor. Reasonable steps could include asking the person to put their request in writing to the home, or asking them to verify existing information that the organisation holds.

d) Staff members should not give out personally-identifiable or company information over the telephone unless they have satisfied themselves as to the identity of the requestor. This should be done as an exception rather than as standard. Most spurious requests for data will come in this way!

e) Staff members should not read out any detail contained in service user records, including the demographic details, over the telephone.

f) Identity Theft is the crime of impersonating someone, using their personal information, for financial or other gain.

g) When faxing personally-identifiable or company information staff members should follow the Caldicott's principles where all faxed confidential information will be managed using the same arrangements.

h) Breaching confidentiality is not just restricted to paper or computer records. Staff members should take care when discussing pertinent cases with their colleagues that the conversation is not being overheard.

i) Staff members should ensure confidential information is destroyed as confidential waste as opposed to being placed in a waste paper bin.

j) Staff members should use organisational shredders. Some shredders also allow CD's to be shredded. This will reduce the risk of confidential data being taken from the waste disposal.

k) Care should be taken by staff members when selecting a printer and sending confidential documents to print if the printer is not located within their own office or if this printer is shared with colleagues. These documents should be collected immediately and not left for others to see.

l) Staff members must take care when photocopying a confidential document that they don't accidentally leave the copy in the photocopier machine.

m) Staff members should always lock their computer workstation if they need to leave it unattended and use a unique pass word to access their computer.

n) Staff members should change passwords at regular intervals and must never write them down, nor share them with any other person, whether a close colleague or otherwise.

o) Computer document shall be disposed of securely when no longer required. Confidential information shall not be leaked to outside persons through inappropriate disposal of computer media.

p) The home processes personally-identifiable data for quality assurance purposes including Staff Training and various audits.

q) For audits, data should be anonymised wherever possible to protect personal data. This may be in the form of coding data or totally removing personal data from the audit.

r) The home also processes personally-identifiable data for conducting service evaluation, in order to develop new knowledge to improve and develop innovative services.

s) Formal Service Evaluation conducted within the home will be required to uphold the same ethical principles (such as gaining informed consent, data protection and confidentiality) as any other data.

t) Staff members should not respond to press enquiries over the telephone. As an alternative please direct the caller the manager who is the only authorised person to talk to the press.

u) Guidance can and should be sought from the manager, deputy manager and the data controller.

v) Staff are prohibited from working with mobile phones whilst on shift and / or taking photographs of service users with their personal smart phones, cameras or i-pads, etc. mobile phones must be locked in their personal lockers whilst on shift.

w) Staff must obtain verbal consent of the service user(s) prior to taking photograph(s) which can be done only using the home's camera and for the purposes of the business / service.

7. Consent

a) Individuals must be effectively informed about ways the information they have provided may be used, to enable them to give their consent (*explicit* / *express* or *implied*) for the disclosure and use of their personal information.

b) ***Explicit, or express, consent*** means articulated agreement. These terms are interchangeable and relate to a clear and voluntary indication of preference or choice, ***usually given orally or in writing and freely given*** in circumstances where the available options and the consequences have been made clear.

c) Implied consent means agreement that has been signalled by the behaviour of an informed person.

d) An informed person should be provided with:

- *a basic explanation of what, why and when information is recorded and what further uses may be made of it;*
- *a description of the benefits from the proposed use or disclosure of information;*
- *an understanding of how the information will be protected, how it is likely to be retained and under what circumstances it will be destroyed;*
- *a knowledge of any outcomes, implications or risks if consent is withheld;*
- *an explanation that any consent given can also be withdrawn in the future.*

ii. People have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them. Decisions to disclose without consent and the justification for disclosing should be noted in the person's records.

iii. ***Staff members should always seek explicit consent from the caller before sending records to the Out-of-Hours providers.***

iv. ***There are situations where consent cannot be obtained directly from an individual due to their lack of capacity at that time.*** In these circumstances it may be possible to seek consent on behalf of the individual from someone else, for example, a family member or other representative. ***Any decision to breach confidentiality must be made in the best interests of the person unable to provide consent.***

v. There are circumstances in which disclosure of information or requests for further information without the individual's consent may be professionally appropriate due to the potential risks involved. If the individual is deemed to have capacity to withhold consent then staff may need to seek advice from Mental Health Professional prior to proceeding without informed consent.

vi. Seeking consent may be difficult if an individual's disability has prevented them from being informed about the likely uses of their information. All individuals must be treated in a fair and equitable manner and reasonable adjustments can be made to ensure information is provided in a suitable format, for example, sign language, interpreter provision.

8. Openness, Transparency and Information Sharing

Information will be made accessible:

- to anyone, in ways that suit their needs and in compliance with Data Protection and Freedom of Information legislation
- to staff where it is necessary for the delivery of their services and the discharge of their duties
- to our partners / other service providers, where it is necessary for the delivery of joint services and in accordance with agreed information sharing protocols.
- Sensitive and confidential information will be shared with other organisations only where there is a need or obligation to do so. Where there is a need to enable service delivery the information sharing will be governed either under the terms of a contract or information sharing agreement. The home will also share information as required by law.
- We will promote to all of our residents, third parties and partners / other service providers our commitment to information security.

9. Employees

a) Pre-employment checks on candidates we are going to appoint for employment and contracts will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements.

b) Confidentiality and Data Protection will be included into objectives and training as appropriate. Personal targets, agreed as part of the appraisal process and, where appropriate, initial job description for employees will include the practice and encouragement of Information Security.

c) All new employees will undergo induction in Confidentiality, Data Protection and Freedom of Information, covering the principles and legal aspects. Subsequently, all employees will be encouraged to undertake further or refresher training as required to maintain safe access to sensitive and confidential information.

10. Handling Information Safely and Breaches of Policy

Any loss of sensitive and confidential information, either actual or suspected, must be reported immediately to the manager or deputy manager. The incident will be handled by the manager.

Where staff or service delivery partners / other service providers have acted in accordance with this policy, but a breach occurs through the action of others, they will be deemed to have acted reasonably. However, if staff are found to be in breach of the policy and its guidance then they may be subject to disciplinary or other appropriate action.

11. Review arrangements

This Policy will be reviewed annually unless an earlier date is agreed by manager.

APPENDIX: Confidential Documents: *Specific Examples*

The following is a list of documentation, which should be treated as confidential when being processed by staff members. This list is indicative and should not be considered as a complete list of confidential data processed by NHS Direct.

HR Documentation

- Personal files;
- Recruitment application forms;
- Employment check and CRB disclosure information;
- Short listing and interview assessments;
- Payroll, pay and contracts documentation and forms;
- Sickness records;
- Disciplinary documentation.

Clinical Documentation

- Care notes / plans
- Handover notes
- Incidents for National Review / Serious Untoward Incident documentation;
- Electronic Health Records;
- Voice recordings;
- Adult Concern Referral documents;
- Special notes information;
- Complaints and Feedback.

Finance Documentation

- Contract information between the company and service user and between the company and other organisations / third parties;
- Travel Expenses Claim Form;
- Remittance Advice;
- BACS records (staff salary/bank details etc);
- Attachment of Earnings Orders;
- Trade Union Membership details (e.g. NMC).

Miscellaneous Documentation

- CCTV recordings;
- Photographs, videos unless prior written agreement has been signed
- Freedom of Information requests;
- Subject Access Requests.

PROCEDURE

1. Handling sensitive or confidential information

The following procedures are set out for all employees and service delivery partners as the *minimum* standards for handling sensitive and confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

a) **Creation/acquisition**

When information is acquired and records created there are some simple principles you must follow. You must ensure that it is:

- ***accurate (factual or qualified expert opinion)***
- ***up to date (changes updated as soon as possible)***
- ***consistent (the same information across different datasets)***
- ***relevant (only as much and for as long as needed for the intended purpose)***

When acquiring and handling personal information you must comply with the processes and standards set out under the Data Protection Act 1998.

b) **Maintenance and use**

Information and records must be maintained to ensure that they are accurate, up to date and consistent. When using sensitive or confidential information there are some ground rules you must follow to maintain confidentiality and integrity:

- ***never leave the information where others could see it e.g. on a desk, computer screen or left on a fax or printer***
- ***do not discuss the information where others not authorised may overhear***
- ***only use the information for the purpose for which it was collected***
- ***changes must be recorded as soon as possible after the change occurs***
- ***always store information securely, following filing procedures in structured file systems***
- ***always put the information/records back as soon as you have finished using them***
- ***do not produce copies unless they are needed and always update the master record, securely destroying copies as soon as they are no longer needed***
- ***review the information regularly to ensure it is accurate and up-to-date***
- ***if information and records are taken from a secure location the risk of loss increases and you must follow the standards set out in the***

c) **Storage**

All sensitive and confidential information must be stored securely and access allowed only to those who need it for legitimate purposes.

Secure storage can be secure buildings with access controls to the building and individual offices. The controls are swipe machines, keypads, key locks etc. Appropriate measures must be used depending on the sensitivity of the information and who should have access to it. Similarly access to electronic information must be controlled by the use of passwords and assigned permissions within the systems that hold the information. To ensure appropriate access under these controls you MUST NOT let others use your access whether it is a key, login or system password or other access control.

d) **Working in non-secure locations**

Some staff may work in locations other than secure company premises i.e. at home, communal lounge in the home where there are service users or visitors. In these cases you must be careful about what you work on and the environment in which you working. The main risks are:

- unauthorised people seeing the data you are working on (particularly in public places)
- information being left on a machine that will be used by others
- information being left where others can find it

- loss or theft of data – unknown disclosure
- in this instances staff should:
  - ☒ ***Never leave paper copies unattended in public places***
  - ☒ ***Always take care to ensure no one can read 'over your shoulder'***
  - ☒ ***Always dispose of information securely (cross shredders are acceptable for this)***
  - ☒ ***Always update the master file promptly (especially if others use it)***
  - ☒ ***Never work on sensitive information on public access devices***
  - ☒ ***Never work on sensitive information on your home PC***
  - ☒ ***Never save sensitive information on the machine***
  - ☒ ***If printing documents ensure you are connected to the correct printer beforehand. This can be a problem with 'roaming profiles'***
  - ☒ ***Keep records at home for as little time as possible.***
  - ☒ ***Records should not be accessible by other family/household members or visitors when working at home.***
  - ☒ ***The employee must ensure that manual information is kept securely, preferably in a locked drawer or locked filing cabinet or room and is not made available to members of the family.***
  - ☒ ***The employee should ensure that when information is unattended, that doors/windows can be secured.***
  - ☒ ***Confidential waste should be shredded before disposal. If this facility is not available at home, then this should be done in an office.***

e) Confidentiality of Records

- The work of this organisation inevitably involves the need to know a good deal about our services users; without access to this information we cannot provide good care
- Much of this information is highly personal and sensitive. We recognise that our individuals have a right to privacy and dignity and, furthermore, that this extends to our handling information about them in ways that intrude as minimally as possible on those rights
- We want our individuals to feel at ease with the staff who help to care for them. An important element in that relationship is the capacity for an individual to be able to share information with staff, confident that it will be used with appropriate respect and only in relation to the care provided
- As providing care is a complex process, it is not possible to guarantee to an individual that information they give about themselves will be handled only by the staff to whom it was first passed; however, we can ensure that information is seen only by staff on the basis of their need to know
- We sometimes have to share information with colleagues in other agencies, but we only do so on the basis of their need to know and, as far as possible, only with the permission of the person concerned
- We will only break the rule of confidentiality in very extreme circumstances that justify taking such action for the greater good of an individual or, exceptionally, others.

f) Our Legal Obligations: Data Protection legislation places various legal obligations on this organisation and similar organisations concerning the handling of the information we hold on individuals. Information must, for example, be obtained fairly and lawfully; be held for specified purposes; be adequate, relevant and not excessive for the purpose for which it was gathered; be accurate and up to date; and be held for no longer than is necessary. We observe all of these requirements.

N.B. Guidance on confidentiality and how it can be maintained in respect of individual information is now assisted by a wealth of information. Refer to the following:

- Records Management Code of Practice for Health and Social Care 2016 published by the Information Governance Alliance
- Department of Health 2003 Confidentiality NHS Code of Practice
- National Institute for Health and Clinical Excellence (NICE)
- Information Commissioner Codes of Practice
- Local authority confidentiality agreements

g) **Information and Care Needs Assessment:** Every user of the services of this organisation must have their care needs thoroughly assessed before services are provided. This necessarily entails the staff who carry out an assessment, or who handle assessment material sent to us from other agencies, learning a considerable amount about an individual. It is the duty of such staff to retain, record and pass to the allocated care workers only the information that is relevant to the person's future care; a similar obligation applies to staff involved in a review or reassessment of care needs or in making any changes in the service provided.

h) **Handling of Information:** The staff assisting an individual have access both to the information passed to them when they start to work with that individual and also to knowledge that accumulates in the course of providing care. They have a duty of confidentiality to do the following:

- ☞ Treat all personal information with respect and in the best interests of the individual to whom it relates
- ☞ Share with their manager, when appropriate, information given to them in confidence
- ☞ Share confidential information, when appropriate, with colleagues with whom they are sharing the task of providing care
- ☞ Pass and receive confidential information to and from colleagues on occasions when they have to be replaced due to sickness, holidays or other reasons, in a responsible and respectful manner
- ☞ Pass confidential information to other social and healthcare agencies only with the agreement of the individual, the permission of their manager, or in emergencies (when it is clear that it is in the interests of the individual or is urgently required for the protection of the individual or another person)
- ☞ Refer to confidential information in training or group supervision sessions with respect and caution and preferably in ways that conceal the identity of the individual to whom it relates
- ☞ Never gossip about an individual or to pass information to any other individual other than for professional reasons.

i) **Managerial and Administrative Responsibilities:** Confidential information must occasionally be seen by staff other than those providing direct care; therefore, it is the responsibility of managers to ensure that information is stored and handled in ways that limit access only to those who have a need to know, and in particular that the following arrangements exist:

- ☞ Lockable filing cabinets to hold individuals' records and ensure that records are kept secure at all times
- ☞ Information held on computers to be accessed only by appropriate personnel
- ☞ Office machinery positioned, with appropriate shielding if necessary, so that screens displaying personal data are hidden from general view.

j) **Exceptional Breaches of Confidentiality:** There are rare occasions in which it is necessary for a staff member acting in good faith to breach confidentiality in an emergency, e.g. to protect the individual or another person from grave danger, without obtaining the permission of the person to whom it applies. In such circumstances, the staff member should use their best judgement; should consult the individual's representative (a manager or a colleague, if possible); and should inform their manager of what has happened as soon afterwards as possible.

The same rules of confidentiality apply to nursing or care records as apply to all personal information concerning individuals. The care plan and other components of the individuals' record are the responsibility of the organisation in respect of the storage, safe custody and destruction of the records. These records may be disclosed by court order to legal, medical or other professional advisors to the individual, either prior to or during legal action.

This organisation is registered with the Information Commissioner's Office (ICO) and complies with *Data Protection legislation*.

k) **Disposal:** When disposing / destroying of any sensitive and confidential information you must comply with the Health and Social Care Act 2008 and CQC's Guidance Essential Standards of Quality and Safety Schedules for the specific information and records being disposed.

When disposing of sensitive and confidential information you must always use secure methods such as cross-cut shredding ***NEVER put sensitive and confidential waste in normal waste bins.***

CQC's Essential Standards of Quality and Safety Guidance states that all relevant to the service records are kept and for the periods of time stated in the table below:

RECORD DESCRIPTION / NATURE OF RECORD	FOLLOWING THE DATE OF LAST ENTRY, RECORD TO BE KEPT *(as ticked below)*			
	18 months	3 years	4 years	Other
Risk Assessments				***retain the latest risk assessment until a new one replaces it***
Purchasing Excluding Medical Devices and Medical Equipment	☑			
General Operating Policies and Procedures		☑ ***Previous version***		
Any Incidents, Events or Occurrences that Require Notification to the CQC		☑		
Use of Restraint or The Deprivation of Liberty		☑		
Detention Under MCA 1983		☑		
Maintenance of The Premises		☑		
Maintenance Of Equipment		☑		
Electrical Testing *(except for 5 years testing)*		☑		
Fire Safety		☑		
Water Safety		☑		
Medical Gas Safety, Storage and Transport		☑		
Money or Valuables Deposited for Safe Keeping		☑		
Staff Employment		☑		
Duty Rosters			☑	
Purchasing of Medical Devices and Medical Equipment				***11 years***
Final Annual Accounts				***30 years***
Public and Employers Liability				***40 years***

2. DATA IN TRANSIT

a) Scope

The scope covers all circumstances where sensitive or confidential data are taken outside of their normally secure location. This includes data in all formats: non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media (i.e. USB memory sticks, PDAs etc.).

b) Responsibilities

The home maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff and members i.e.:

- Secure network for storing and using electronic data
- Secure work locations for storing and using hard-copy data
- Encryption tools for transmission of data outside secure locations

Where data sharing protocols and agreements are already in place for your service area (e.g. the Sussex Police, Multi-Agency Data Sharing Agreement) you must act in accordance with the security standards specified in such agreements where they exceed those of this policy. In all other respects you must work to the standards set out in this policy.

c) 'Common Sense' Precautions

There are some 'common sense' precautions that you can take before sending or taking sensitive or confidential data outside of their normally secure location, these are:

- ***Check that you are not sending / taking more details / information than is necessary i.e. will the information still meet the need if you remove the sensitive material or aggregate the data?***
- ***Check that the data you are sending / taking are correct and appropriate.***
- ***Check that you are sending the data to the correct person / address.***
- ***Check how you intend to keep it secure.***

The following methods are ranked in categories of security and preference and it is your responsibility to ensure that you use a method and degree of security appropriate to the sensitivity, quantity and potential impact of the data being handled.

- Make sure the recipient is known and trustworthy
- Make sure it is traceable (apply delivery and read receipts) where possible

d) Web Portal

If you are transferring sensitive or confidential data through a web portal you must:

- Ensure that there is robust access control in place (i.e. unique username/password)
- Ensure that only the people who need the data can see them
- Ensure that the data are encrypted (https connection)

e) Mobile Storage Devices

If you are taking data with you on a mobile storage device, *such as a tablet PC, laptop or a USB memory stick, they must be encrypted and you must:*

- ***Make sure that there is no other more secure option available to you***
- ***Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible***
- ***Keep the decryption password/token securely and separately from the device/data***
- ***Take all reasonable precautions to keep the device and data safe and secure e.g.:***
  - ***Keep it with you whenever possible; lock it away securely when you can't***
  - ***Never leave it in plain sight in public places***
  - ***Never let others use your access or device***
  - ***Delete the data from the device as soon as possible***
  - ***Report loss/theft immediately***

l) **Post**

The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data. There are precautions that you must take to prevent loss:

- Check that more secure alternatives are not available
- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Make sure it is traceable (i.e. confirmation of receipt)
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

m) **Home PC / laptop**

If you are working at home on your own PC or laptop you must:

- Only have as much sensitive or confidential information open as necessary and only for as long as necessary – do not save the data on your machine and do not leave the gateway connection open when you are not actively working on it
- Always save the data back to their normally secure location when you have finished

- ☞ You must not leave the computer unattended for any period of time such that others can access any sensitive data; always lock the computer or log out when you are not using it

n) **Physical (Paper) Records**

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

- 👍 Make sure that there is no other option available to you
- 👍 Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- 👍 Take only as much as necessary and only for as long as necessary
- 👍 Transfer it back to its normally secure location as soon as possible
- 👍 Take all reasonable precautions to keep the records safe and secure e.g.:
- 👍 Keep them with you whenever possible; lock them away securely when you can't
  - ➢ Use a suitable container that prevents accidental loss and/or viewing by others
  - ➢ Never leave them in plain sight in public places
  - ➢ Report loss/theft immediately

o) **Fax**

Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

- 👍 Check that more secure alternatives are not available
- 👍 Make sure the receiving fax machine is in a secure environment
- 👍 Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
- 👍 Make sure it is traceable (e.g. confirmation of receipt)

p) You must not!

There are some data handling activities which simply must be avoided:

- 👎 **Sending sensitive or confidential information as unsecured physical records.**
- 👎 **Working on sensitive or confidential data on a public PC / laptop (for example in a library or cafe).**
- 👎 **Working on sensitive or confidential data on a PC or laptop with an unencrypted wireless (WiFi) connection, i.e. ensure your home wireless network has encryption and use it.**
- 👎 **Leaving sensitive or confidential physical records in plain view of others (i.e. on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).**
- 👎 **Leaving any device holding sensitive or confidential information unattended in plain view of others.**

3. Reporting Data Loss

- ☞ In the first instance staff should report a loss of sensitive and/or confidential data to their manager or deputy manager.
- ☞ The manager or deputy manager will determine the significance of the loss and will take appropriate action.
- ☞ The manager or deputy manager will investigate the circumstances of the loss and will be responsible for taking corrective action to prevent re-occurrence.
- ☞ Any loss must be reported using the incident reporting procedure.
- ☞ To be reported to ICO within 72 hours

4. Methods of data transit and storage

a) The following is a ***list of methods and devices commonly used to store and/or transfer data*** outside of their normally secure location.

- ☞ Email
- ☞ Fax
- ☞ Post
- ☞ Mobile devices:

- ☞ Laptops and tablet PCs
- ☞ CD/DVDs
- ☞ PDAs - IPAQs
- ☞ Smartphones
- ☞ Mobile Phones
- ☞ USB flash/hard drives - memory sticks
- ☞ Cameras, dictaphones
- ☞ Home PC/laptop
- ☞ Public PC/laptop (e.g. in a library or cafe)

b) **Normally Secure Location:** For the purposes of this policy standard 'normally secure location' is defined as:

- ☞ A secure network/storage facility with:
  - ☑ Access controls such as individual login accounts
  - ☑ Backup and recovery facilities
  - ☑ No public access
  - ☑ Anti-virus and firewall protection

c) Encryption/Decryption

Encryption is the process of transforming information to make it unreadable by anyone who does not have an appropriate 'key' or 'token'. Those who have an appropriate key or token can use it to reverse the encryption process (known as decryption) to enable them to read the information.

d) **Last Word: Remember:**

If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone what would you do to protect it?

5. Handling Security Incidents Affecting Confidential Information

a) **Introduction:** There are several ways in which confidentiality may be breached such as theft, break-ins, unauthorised disclosure, correspondence being sent to incorrect recipients (e.g. incorrect email address used or fax number being dialled), loss or poor disposal of confidential waste. All breaches should be investigated and reported accordingly. This procedure provides mechanisms for handling security incidents where confidentiality has been or may have been breached and must be reported to the manager or deputy manager.

The majority of information security breaches are innocent and unintentional such as the user not 'logging out' at the end of the day or documents left out on a desk. However, 'near misses', where no actual harm results from the incident, should still be reported to the manager or deputy manager and analysed to look for possible ways of preventing a harmful incident occurring in the future.

b) **Types of security incident**

The types of security incidents likely to breach confidentiality are variable. Information security incidents may take many forms including the following:

- ☞ Theft of equipment holding confidential information – e.g. PCs, case notes, portable storage devices such as USB sticks
- ☞ Unauthorised access to a building or areas containing unsecured confidential information
- ☞ Access to service user records by an authorised user who has no work requirement to access the records
- ☞ Authorised access which is misused
- ☞ Unauthorised electronic access (hacking) and viruses
- ☞ Misuse of equipment such as faxes, text messages on mobiles and e-mails
- ☞ Inadequate disposal of confidential material - e.g. paper, PC hard drive, disks/tapes
- ☞ Car theft / break-ins
- ☞ Unauthorised access to records away from premises (e.g. laptops and notes when travelling etc.)
- ☞ Complaint by a service user, or a member of the public, that confidentiality has been breached
- ☞ Indiscrete disclosure of information, including abuse of social media
- ☞ Software malfunction
- ☞ Data corruption

- ☞ Accidental deletion/destruction, and
- ☞ Loss of information or any equipment or media containing information.

c) **Reporting arrangements**

- ☞ All incidents or information indicating a suspected or actual data security breach must be reported immediately to your line manager.
- ☞ It may also be necessary to report the incident to the Police immediately depending on the type and likely consequences of the incident.
- ☞ Incidents should always be investigated immediately while there is still the possibility of collecting as much evidence as possible.

d) **Implementation of the Information Breach Management Plan**

However the breach has occurred, there are four important elements to any breach management plan which must be considered immediately by the manager or deputy manager:

- ***Assessment of impact and ongoing risks***

  Assess the impact and ongoing risks which may be associated with the breach. Most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

- ***Containment and recovery***

  Information security breaches will require not just an initial response to investigate and contain the situation, but also a recovery plan including, where necessary, damage limitation.

- ***Notification of breach within 72 hours***

  Informing people and organisations that we have experienced an information security breach may be an important element. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to provide advice and deal with complaints.

- ***Evaluation and response***

  It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response to it. If the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. If the response was hampered by inadequate policies or a lack of a clear allocation of responsibility, then it is important to review and take remedial action.

e) **Disciplinary investigation**

- ☞ Staff members are encouraged to report all information security incidents immediately they occur to the manager or deputy manager. It is crucial that incidents are contained and everything appropriate is done as soon as possible to limit the damage to individuals for whom confidentiality has been breached. Failure to report incidents could have serious consequences for individuals' welfare and personal safety, particularly if the compromised information is sensitive.
- ☞ The decision for a disciplinary procedure should be taken only after appropriate investigation of establishing the facts has been undertaken.
- ☞ Where formal action is deemed necessary, a separate disciplinary investigation will be carried out in line with the Disciplinary Policy and Procedure. This will be confidential and independent of the information breach management process.

SOCIAL MEDIA: FACEBOOK, TWITTER, TUMBLR, BLOG, SKYPE, SMART PHONES, ETC. AND OTHER INVENTIONS OF THE INFORMATION TECNOLOGY ERA:

In a word: NO!! NO!! NO!! NO!! DEFINITELY NOT!!!!!!!!

1. Facebook and Twitter: on – line social networking services

Point 2 of 'Facebook' Terms of Business states:

"*2. Sharing your Content and Information*

.....

1. *For content ..... like photos and videos ...., you specifically give us the following permission, ...: you grant us a non – exclusive, transferable, sub – licensable, royalty – free, worldwide license to use any IP content that you post on or in connection with Facebook.*
2. *.....*
3. *.....*
4. *When you publish content or information ....., it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).*"

In other words: it is evident from Facebook Terms of Business that **there is no confidentiality and / or privacy on Facebook or Twitter. Once something is published on Facebook or Twitter, it is out there for everybody to read and see!!! And it is never really deleted as backup copies exists!!!** For example: One day a teacher in a prestigious school had a discussion with some parents. Later on when she went home, she wrote and published her opinion on Facebook (which was not complimentary, quite the opposite, she used words like 'silly', etc.), about the parents and set it up so that only her friends could access it. However, some of the parents read the teacher's comments and complained. The teacher was later on dismissed and she could not find a job. Facebook representative told her that she should have read the Terms of Business. **As a result of an indiscretion on Facebook, the teacher's whole life was pulled apart.**

Therefore, staff MUST NOT write, discuss, comment or publish anything on Facebook, Twitter, newspapers' / magazines' websites, e-mails, Skype, Blog, Tumblr, etc. including photographs and / or videos about:

- 👎 **Service users and / or**
- 👎 **Their families, friends, representatives, LPAs, pets, belongings, etc.**
- 👎 **Other visitors such as professionals: GPs, Social Workers, Dieticians, etc.**
- 👎 **The home, including the building outside, inside or the garden (front and back), the regulated activities, facilities, equipment, records, etc.**
- 👎 **Other staff, names, age, occupation, sexual orientation, etc.**

2. Smart Phones: This organisation recognises its responsibility to ensure that all reasonable precautions are taken to provide and maintain working conditions that are safe, healthy and compliant with all statutory requirements and codes of practice. This organisation recognises that the personal use of mobile phones in the workplace can be disruptive, affect concentration and efficiency, and may therefore jeopardise the safety of residents, the home and its reputation.

a) STAFF MUST NOT:

- 👎 **Must not work with their personal mobile or smart phones; must not have their mobile or smart phones on them whilst on shift.** Phones should be locked in the staff personal lockers for the duration of their shift.
- 👎 **Must not take any photographs of the service users, their families, friends, pets, etc. with smart phones.**
- 👎 **Must not take any photographs of the home including the building outside, inside or the garden (front and back), the regulated activities, facilities, equipment, etc.**
- 👎 **Must not take photographs of any records related to service users, staff or the home / business.**
- 👍 **Photographs of the service users can only be taken with their expressed permission, verbal or written consent for occasions such as Birthdays, Open Days, activities, etc. with the home's camera only.**
- 👍 **Mobile phones and charging cables brought into the home for work or personal use must be in good condition. Cables must be intact and free from damage. If, when in use, faulty**

equipment or leads are seen, the staff member will be asked to stop using it immediately and the lead unplugged.

The monitoring of charging leads in use will form part of the electrical safety monitoring procedure in the home.

b) Emergency Contact Considerations

- ⚠ The employee can be contacted in an emergency on the residential home's telephone number
- ⚠ The employee can give out the organisation number to spouse, school and relatives
- ⚠ The employee is allowed to use their personal mobile phone for emergency calls
- ⚠ On some occasions an employee may request and discuss in advance with the manager that they are allowed their mobile phone switched on (on a vibration) at work for a specific reason. Each request will be considered and judged on its own merits by the manager.

c) Specified Areas for Usage

- ✓ Outside company buildings
- ✓ Staff room and smoking areas.

1. Disciplinary action: Staff members who are in breach of the rules set above in section 1 and 2 in relation to Facebook, Twitter and other on – line social media, and smart phones will be investigated and be a subject to:

a) Disciplinary policy and procedure and / or

b) Safeguarding investigation

SOCIAL MEDIA: In a word:

NO!! NO!! NO!! NO!! DEFINITELY NOT!!!!!!!!

NOT A WORD, NOT A PHOTO, NOTHING!!!

Further Guidance

A guide to confidentiality in health and social care published by the Health and Social Care Information Centre September 2013:

- *Code of Practice on confidential information published by the Health and Social Care Information Centre December 2014*
  http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

- *Confidentiality – Nursing and Midwifery Council (NMC):*
  http://www.nmc-uk.org/Nurses-and-midwives/Advice-by-topic/A/Advice/Confidentiality/

Related Policies

Co-operating with other Providers
Consent
Corporate Social Responsibility
Cyber Security
Data Protection (GDPR)
Good Governance
Record Keeping