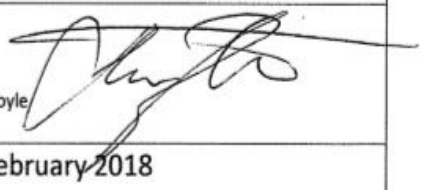
PRIVACY POLICY

POLICY NUMBER	OP00090
AUTHOR	Margaret Mary Cowan
APPROVED BY	Gordon McHugh
IMPLEMENTATION DATE	16 February 2018
REVIEW DATE	February 2021
VERSION	V1.0
RATIFIED BY	John Doyle 
DATE RATIFIED	16 February 2018

AMENDMENTS

Version	Amendment date	Author	Ratified by

PRIVACY POLICY

POLICY NUMBER	OP00090
AUTHOR	Margaret Mary Cowan
APPROVED BY	Gordon McHugh
IMPLEMENTATION DATE	16 February 2018
REVIEW DATE	February 2021
VERSION	V1.0
RATIFIED BY	John Doyle
DATE RATIFIED	16 February 2018

AMENDMENTS

Version	Amendment date	Author	Ratified by

1. The Duty of confidence

The Hospice has a duty of confidence to patients and a duty to support professional ethical standards of confidentiality.

Everyone working for or with the Hospice records, handles, stores or otherwise comes across information that is capable of identifying individual patients. All have a personal duty of confidence to patients and to his/her employer.

The duty of confidence is conferred by common law, statute, contract of employment and professional registration.

This Policy is primarily but not exclusively concerned with patient confidentiality. The principles apply equally to information regarding other individuals, including staff, volunteers, customers and fundraisers.

The purpose of this policy is to ensure everyone in the Hospice is aware of the importance of confidentiality, and their responsibilities for safeguarding confidentiality and keeping information secure. This policy should be read in conjunction with the Kilbryde Hospice Information Governance policies.

2. Responsibility/Accountability

Overall responsibility:	Chief Executive Officer
Specialist Responsibility:	Caldicott Guardian
Line Responsibility:	Line/Dept. Managers
Individual Responsibility:	All staff and volunteers

As well as holding overall responsibility for the adherence of Kilbryde Hospice to this policy, the Chief Executive Officer is responsible for appointing the Caldicott Guardian.

The Caldicott Guardian is responsible for overseeing and advising on issues of confidentiality and information protection for the Hospice

Managers are responsible for ensuring that all staff, including temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information.

All staff are responsible for adhering to this Policy and following the associated guidelines, and for safeguarding the confidentiality of all personal and Hospice information, transmitted or recorded by any means.

Breaches of confidentiality are a serious matter. Non-compliance with this policy may result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so.

3. Related Hospice Policies

Staff must comply with the requirements of the Caldicott Report (see Guidelines Appendix 1), current data protection legislation and Kilbryde Hospice Information Governance policies. Please also refer to Kilbryde Hospice Code of Conduct and Volunteer Handbook.

4. Procedure(s)

What is personal sensitive data?

Current data protection legislation defines personal data as any information relating to an identified or identifiable natural person (data subject). Identification can be made by name, identification number, location data, on-line identifier to one or more factors specific to their physical, psychological, genetic, mental economic, cultural or social identify".

For the purposes of current data protection legislation, identifiable means by using "all" means IP addresses, cookies and RFID tags.

- Confidential information is information entrusted by an individual in confidence, where there is a general obligation not to disclose that information without consent.
- Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive information regarding race, health, sexuality, etc.
- Confidential information may be known, or stored on any medium. Photographs, videos, audio recordings etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.
- Person-identifying information (i.e. that which identifies individuals personally) is assumed to be confidential, and should not be used unless absolutely necessary. Whenever possible anonymise data, from which personal details have been removed and which therefore cannot identify the individual, should be used instead. Note however that even anonymised information can only be used for justified purposes

4.1 Acting on the duty of confidentiality

- Patients are informed of their rights in relation to how the hospice handles confidential information through a leaflet "Your information and how we use it" available at the Hospice and via our website.
- No personal information, given or received in confidence, may be passed to anyone else without the knowledge and consent of the provider of the information. This is usually the patient but sometimes another person (e.g. relative or carer) may be the source.
- No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.
- Patients have the right to object to the use of their personal health data for purposes other than their immediate care.
- The duty of confidentiality owed to a deceased patient should be viewed as being consistent with the rights of living individuals.

4.2 Disclosing information

Information concerning individuals may be passed on to someone else only:

- on a 'need to know' basis;
- when the disclosure is necessary for the clinical care of a patient (e.g. between members of a clinical or multidisciplinary team);
- when required for the safe and effective management of the Hospice and its services e.g. audit and dealing with complaints
- There is a statutory or legal obligation to do so.

In most instances, information may only be disclosed with the patient's consent. The Hospice has an obligation to ensure that its patients are fully informed regarding the uses to which it puts information gathered about them. Provided that patients have been so informed, staff may normally disclose information where this is in the best interests of the patient (e.g. for routine clinical care). However, a patient with capacity may refuse such disclosure, and where there is reasonable doubt, the patient should be asked and refusal of consent must normally be respected.

Certain statutory and legally-required disclosures may not require consent, although the patient must always be informed when such a disclosure is made.

5. Compliance with Policy

All cases of suspected breaches of confidentiality are investigated, decisions reached and investigative procedures documented by the Senior Management Team and Caldicott Guardian.

6. References / Associated Standards / Guidelines

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patients Act 1988

- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Human Rights Act 2000
- NHSiS ITSecurity Manual
- A Manual for Caldicott Guardians 2017
- NHS Scotland Code of Practice: Protecting Patient Confidentiality 2012
- Privacy and Electronic Communication Regulations 2003
- Public Records Scotland Act 2011
- Regulation of Investigatory Powers Act 2000
- Scottish Government Records Management: NHS Code of Practice (Scotland) 2012
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- December 2016 Introduction of new FOI tool (voluntary sector)

7. Appendices

1 Caldicott: legal & professional requirements
2 Third party enquiries
3 Your Information and how we use it (Kilbryde Hospice Leaflet)
4 Right of access information pack

Kilbryde Hospice - Confidentiality Guidelines

Introduction

Under current data protection legislation sensitive personal data relates to the following subject matter

- Health
- Racial or ethnic origin
- Religious beliefs
- Genetic and biometric data
- Sexual orientation

- Everyone working for or with the Hospice who records, handles, stores or otherwise comes across sensitive personal data that is capable of identifying an individual patient, has a personal duty of confidence to that individual and to his/her employer.
- These Guidelines aim to stress the main principles behind maintaining confidentiality. Further guidance may be obtained from the General Medical Council, NHS Scotland and NHS Scotland Code of Practice: Protecting Confidentiality 2012.
- Whilst primarily though not exclusively concerned with patient confidentiality, the principles reflected in these guidelines apply equally to information regarding other individuals, including staff.

Disclosure of confidential information

- When information is passed from one to another, it is said to have been disclosed to the recipient. Good practice in maintaining confidentiality is mainly about ensuring that patients are aware when and why disclosures occur, and that such disclosures are necessary, appropriate, and undertaken safely and securely.
- In many situations it may not be strictly necessary to disclose the identity of the patient. For example, it is often sufficient to communicate or discuss just the clinical details in order to obtain advice about management of a particular patient.

Inappropriate disclosure

- Inadvertent or inappropriate disclosure of confidential information is potentially a serious matter. Adherence to the following principles will reduce the risk of this occurring.
- If you are uncertain whether information is confidential or not, assume that it is.
- Whenever possible, remove person-identifying details (e.g. name and address) and use other information such as the CHI number or Crosscare number.
- Do not give out information unless you are certain that the requestor has a right to receive it. Be especially careful on the telephone: always check the identity of the caller and the individual about whom they are enquiring. Do not automatically assume that they have a right to the information.
- Do not talk about confidential matters where you can be overheard, e.g., near another patient, in the queue at the canteen, in a lift, etc. Be careful not to leave or inadvertently display confidential notes in public places.
- Never look up patient information systems case notes or Crosscare unless you need to know because of your involvement in the care of the patient. For example, you must not look up information on family, friends, celebrities or indeed anyone else out of either curiosity or because you have an interest in doing so outside any clear professional duty of care to that patient.
- Always check fax numbers yourself with the intended recipient before you send

information by fax. Use safe haven areas (located in Admin) and call to say the information is being sent.

- Make sure that case notes and other confidential papers cannot be overlooked or accessed by unauthorised personnel and that computer screens are not situated where they can be viewed by unauthorised personnel
- Make sure that less obvious sources of person-identifying data, such as notebooks, diaries, appointment books, etc. are kept securely, and disposed of when they are no longer required.
- Do not taken any patient data home: the Hospice is still responsible for the data and it must be kept secure at all times.
- E-mail systems are inherently insecure: do not send confidential information by e-mail unless absolutely necessary and only if encrypted. Please refer to Kilbryde Hospice Acceptable Email Usage policy (KH OP0070) for more information.
- Confidential papers must be securely packaged if they are to be transported or sent to another location. Please refer to Kilbryde Hospice Records Management Policy (KH OP0062) for more information.
- Always dispose of confidential material by the proper means. Papers must be put in designated confidential waste bags or bins, and sent for shredding. To dispose of information stored on computer disks, call our current IT support for advice.

Relatives and friends

- In most circumstances, patients will usually want close relatives to be informed about their diagnosis and care, but this may not always be the case and relatives and friends do not have the right to any information about a patient without that patient's consent.
- In the case of patients with capacity it is important that staff discuss with the patient who, if anyone, they wish to be kept informed. In the case of patients who lack capacity to consent to this, staff have a general obligation to act in the patient's best interests and this will normally mean that staff will need to discuss confidential matters with one or more close relatives or friends. The substance of such discussions should be documented in the patient's records, and regularly reviewed and updated. See the **Adults with Incapacity (Scotland) Act 2000**
- In the case of minors (i.e. In Scotland those aged under 16 years) who lack capacity to consent to disclosure, staff should normally inform parents/guardian (strictly those with parental responsibility) of all information relevant to the care and management of the patient. Staff will need such parental consent in order to care for the patient. Patients aged 16 and over who have capacity normally have the right to determine who should know confidential information about them.

Disclosure in the public interest

- Disclosure of personal information without consent may be justified where failure to do so may expose the patient or others to risk of death or serious harm. Where third parties are exposed to a risk so serious that it outweighs the patient's privacy interest, you should seek consent to disclosure where practicable. If it is not practicable, you should disclose information promptly to an appropriate person or authority. You should generally inform the patient before disclosing the information.
- Such circumstances may arise, for example:
  - Where a colleague, who is also a patient, is placing patients at risk as a result of illness or other medical condition. If you are in doubt about whether disclosure is justified you should consult an experienced colleague, or seek advice from a professional organisations. The safety of patients must come first at all times.
  - Where a patient continues to drive, against medical advice, when unfit to do so. In such circumstances you should disclose relevant information to the medical adviser of the Driver and Vehicle Licensing Agency (DVLA) without

delay.

- Where a disclosure may assist in the prevention or detection of a serious crime. Serious crimes, in this context, will put someone at risk of death or serious harm, and will usually be crimes against the person, such as abuse of children.

- Such disclosures must be made in good faith, in the belief that the information is true, and where the disclosure is not made for personal gain.

Disclosure to the Police

- There is no absolute requirement to disclose, or not to disclose information to the police. NHS guidance is that information should be disclosed to assist the police with the prevention or detection of serious arrestable offences.
- Although there is no absolute definition of serious crime, the criminal evidence Act 1984 lists serious arrestable offences as:
  - treason, murder, manslaughter, rape, kidnapping, certain sexual offences, causing an explosion, certain firearms offences, hijacking, causing death by reckless driving, offences under prevention of terrorism legislation;
  - where a court order is presented requiring the information;
  - where a threat is made, which if carried out would be likely to lead to death or serious injury, substantial financial gain or loss, serious interference with the administration of justice or investigation of an offence.

Other disclosures

For other situations, such as disclosures to the Press and media, Solicitors, and disclosures required under Statute (i.e. by law) please see Appendix 3.

People are entitled, under current data protection legislation, to view information about themselves and to have copies of it if they wish (a Right of Access Request). There are some restrictions to the release of information. Information must be provided without delay and at the latest within one month of receipt. Appendix

- You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

- There is no charge for this service although Kilbryde Hospice can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The hospice can also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

- By law, people must be given an explanation of any terms or abbreviations that are not easy for a layman to understand.

- Staff should ensure that all relevant facts and discussions are recorded; however the information should always be defensible. Including colloquial expressions of opinion about patients is most unwise.

Incidents and breaches of confidentiality

- If you think that confidential information may have been revealed by accident, or by other means (for example theft of papers or a computer), it is essential that you complete a Kilbryde Hospice Information Security Incident Notification.

This enables monitoring of information incidents as a whole, and investigation of individual incidents where necessary. It is an important part of ensuring that practice improvements are brought in where necessary, and improving the service for patients.

General data protection principles under current data protection legislation

1. Personal data shall be processed

- Lawfully
- Fairly
- Transparently

2. Personal data shall be collected for

- Specific, explicit legitimate purposes
- Not further processed incompatible with initial purpose

3. Personal data shall be

- Minimised
- Adequate
- Relevant
- Limited to the purpose for which they are processed

- Accurate and kept updated
- Scrutinized for inaccuracies and rectified without delay
- Minimised to a form which permits identification of data subjects for no longer than necessary

- Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing

- Data subjects also have the right to erasure of their personal data (the right to be forgotten) e.g. a person withdraws their consent on which data processing is based.
- Kilbryde Hospice is responsible for and are able to demonstrate accountability with the data protection principle through the Information Governance Group. Kilbryde Hospice will have access to a Data Protection Officer (person still to be appointed).

Dealing with children's personal data under current data protection legislation

These provisions apply to people under 16. Kilbryde Hospice has an obligation to obtain and use reasonable efforts to verify and ensure parental consent when processing personal and sensitive data in relation to children under 16 on the grounds of legitimate interest. Similarly these guidelines will apply for any online services that we will use in the future.

Right of Access

Right to be forgotten

Under current data protection legislation the right to be forgotten has become law. A patient, family member, donor, volunteer or staff member can request erasure of their personal data. (Article 17 current data protection legislation)

- When personal data is no longer necessary in relation to the purposes for which they are collected
- There are no legitimate grounds to process the data
- The person withdraws consent on which the processing is based
- The person's data has been illegally processed

Further information

- Department of Health. The NHS Confidentiality Code of Practice. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAnd Guidance/DH_4069253

- General Medical Council. Confidentiality: Protecting and Providing Information. http://www.gmc-uk.org/guidance/current/library/confidentiality.asp

- Kilbryde Hospice Information Governance Policies

- Adults with Incapacity Act (2000)

- General Data Protection Regulations (2018)

Appendix 1: Caldicott, legal and professional requirements

Caldicott principles

1. The Caldicott Report was commissioned by the Chief Medical Officer in 1997, in response to growing concerns about the risk to patient confidentiality with the increasing use of computers in healthcare.

2. The report contains 16 recommendations, and 6 good practice principles. NHS organisations have to report annually on their progress towards Caldicott compliance against 18 headings (which do not correlate directly with the recommendations or the principles).

3. The Hospice is obliged to appoint a senior clinical member of staff to act as Caldicott Guardian for the Hospice, to oversee issues of confidentiality. The Caldicott Guardian for the Kilbryde Hospice is the Clinical Services Manager.

4. The six Caldicott principles are:

Principle 1	Justify the purpose for each use/transfer of patient-identifiable Information.
Principle 2	Don't use patient-identifiable information unless it is absolutely necessary.
Principle 3	Use the minimum necessary patient-identifiable information.
Principle 4	Access to patient-identifiable information should be on a strict need-to –know basis.
Principle 5	Everyone with access to patient-identifiable information should be aware of their responsibilities.
Principle 6	Understand and comply with the law.

Appendix 2: Third Party enquiries and disclosures

1. Press and Media: No member of staff should attempt to answer questions from any media organisations or individual, but should refer all press and media enquiries to the Chief Executive Officer

2. Solicitors and Legal Representatives: Solicitors acting on behalf of patients have some rights of access to information for their clients. Do not disclose any information yourself, but refer them to the Medical Director or Caldicott Guardian

3. Complaints about Treatment or Care: Formal complaints from patients, relatives or others should be directed to: Chief Executive Officer, Kilbryde Hospice, McGuinness Way, East Kilbride, G75 8GJ.

Mandatory disclosures and disclosures under statute

Bodies empowered to order disclosure

- A Court of Law and Industrial Tribunals
- Health Service Commissioner
- Health and Safety Commission
- Health and Safety Executive
- Inquiries appointed by the Secretary of State
- Employment Medical Advisers
- Professional bodies of the Health Professions – doctors, dentists, nurses, midwives, health visitors, opticians and professions allied to medicine (but not pharmacists)
- Mental Health Act Commission
- Mental Health review Tribunals
- Disclosures to non-NHS organisations such as social services may be essential to the continuing care of the individual but must be strictly controlled.

Additional categories: No information should be disclosed to the following agencies unless in exceptional circumstances, or with the consent of the patient.

- Department of Social Security (DSS / Benefits Agency). The patient's consent must be obtained before notifying the Benefits Agency of their stay in hospital.
- Employers
- Schools
- Police

Appendix 3

"Your information and how we use it" leaflet

Your personal health information

- Kilbryde Hospice staff will record information about you, your medical treatment and family background on paper and computer to form part of your health record.
- With your consent members of the Kilbryde Hospice team including students may share this information with each other and other healthcare professionals so we can work together for your benefit.
- ALL staff working and training in Kilbryde Hospice are bound by law and a strict code of confidentiality and are regulated and monitored by Kilbryde Hospice's Caldicott Guardian (a role responsible for ensuring patients' rights to confidentiality are respected).
- We do not sell, trade, lease or rent your personal information to any other organisations

- **How your records are used to help you**
- The staff involved in your treatment need to have accurate and up-to-date information to assess your health.
- Your records allow hospital staff to assess and investigate the type and quality of care you have received.

How your information can help Kilbryde Hospice

- To review your care to ensure it is of the highest quality
- For reporting to Healthcare Improvement Scotland
- For education and research
- To enable funding applications
- To support the investigation of any incidents or issues that arise.

Sharing your information

- When we are required to share data at your request
- Kilbryde Hospice is legally required to share information e.g. infectious disease outbreak
- Where a formal court order has been issued.

Your information rights

- You have the right to know how we will use your personal information.

- You have the right to access your Health Record
- You have the right to object to us making use of your information.
- You can ask us to change or restrict the way we use your information and we are obliged to agree if it is possible to do so.
- You have the right to ask for your information to be changed, blocked or erased if the information we are holding about you is incorrect.

To make a Right of Access Request

- If you are an inpatient at Kilbryde Hospice, you may ask to look at your Health Record folder. Your notes will be prepared for your viewing and a qualified member of staff will talk you through its content.
- You should be aware that in certain circumstances your right to see some details in your health records may be limited - for example if it would reveal third-party information.
- If you would like to see your Health Record after you leave Kilbryde Hospice, or if you would like copies of your Health Record, you will need to send a written request, called a Right of Access Request, to the Chief Executive Officer. Please request this from a senior staff member.

Kilbryde Hospice Data Controller
Mr. Gordon McHugh
Chief Executive Officer
Kilbryde Hospice
East Kilbride
G75 8GJ

Appendix 4:

Right of Access Request

Kilbryde Hospice reminds all employees that people ("data subjects") have the right to request access to personal information about them.

We are committed to providing people access to information whenever possible and appropriate.

Current data protection legislation gives people the right to know what we are doing with their personal information and to receive a copy of the personal data so that they can ensure that the information is being used properly and is accurate. This is called a Right of Access Request.

The Hospice's Privacy Policy states that all individuals have the right to request access to personal sensitive information about them. We are committed to providing applicants access to information wherever possible and appropriate. We must provide the individual with his or her personal data unless some or all of the personal data can or must be withheld in terms of one or more of the exemptions set out in the current data protection legislation.

Under the current data protection legislation**,** individuals will have the **right** to obtain: confirmation that their data is being processed; **access** to their personal data; and. other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (Article 15).

This section gives people the right to "access" their personal data.
Current data protection legislation Article 15 states;

- People have the right to modification of their personal data
- People have the right to access their personal data
- People have the right to object to processing of personal data
- People have the right to not be subject to automated decision taking
- People have the right to transparency
- People have the right to data portability(receive a copy themselves or have it sent to a third party
- People have the right to erasure of personal data (the right to be forgotten)

Under current data protection legislation Kilbryde Hospice will explain if requested

- The purposes of processing the data
- The categories of data processed
- The recipients or categories of recipients (in particular international organisations)
- The envisaged retention period of data
- The individual's rights of modification or erasure of data to restrict processing
- Information regarding the source of the data (if not collected from the data subject)

A Right of Access Request should only be refused if it is clearly for a different purpose e.g. obtaining information for a court action against Kilbryde Hospice.

Dear

Current data protection legislation 2018
Right of Access Request

Thank you for your enquiry on *[insert date]* regarding requesting personal information from Kilbryde Hospice.

To assist you in making your request, which must be made in writing, here is a guidance note and an information request form. It would be helpful if you use the form to make your request, but you can also make your request in a letter.

You can hand your request in to Kilbryde Hospice or post it to the address above. There is no charge for this service however the hospice reserves the right to charge if there are repeated or subsequent access requests.

Proof of identity

Please note that Kilbryde Hospice requires proof of your identity to ensure that they are dealing with a request from the appropriate person.

Kilbryde Hospice would like copies of at least two different forms of proof of identity (I do not need to see the originals). The guidance and request form provides some more information. If I do not receive proof of identity the Hospice will be unable to process your request.

Exempt Information

There are times when we will hold back information from you. We will only hold back information in when the current data protection legislation permits us to do so. If this is the case, we will explain to you why we are not giving you the information. We will give you details on how to complain about any decision to hold back information. At all times we will seek to provide as much information as possible.

If you require further information or assistance, please do not hesitate to contact me.

Yours sincerely,