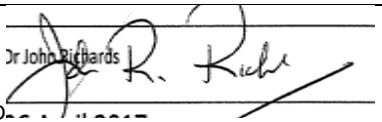
# CONFIDENTIALITY POLICY

| | |
|---|---|
| **POLICY NUMBER** | OP00023 |
| **AUTHOR** | Margaret Mary Cowan |
| **APPROVED BY** | Dr Hosney Yosef |
| **IMPLEMENTATION DATE** | 26 April 2017 |
| **REVIEW DATE** | 25 April 2020 |
| **VERSION** | V1.0 |
| **RATIFIED BY** |  r John Richards |
| **DATE RATIFIED** | 26 April 2017 |

**AMENDMENTS**

| Version | Amendment date | Author | Ratified by |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**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 and volunteers.

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 Hospice Data Protection Policy.

## 2. Responsibility/Accountability

| | |
|---|---|
| Ultimate Responsibility: | Chief Executive |
| 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 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), the Data Protection Act 1998 (see Guidelines Appendix 1), The NHS Confidentiality Code of Practice, the Hospice Data Protection Policy and Management of Patient Information Policy and Guidelines, the Hospice staff/volunteer code of practice and professional codes of practice .

1. Data Protection Policy
2. Management of Patient Information
3. Consent to Treatment
4. Protection of Children Policy
5. Protecting and Supporting Adults at Risk of Harm
6. Risk Management Policy
7. Accident and Incident Reporting Policy
8. Complaints Policy
9. Whistleblowing Policy
10. Disciplinary
11. Grievance
12. Hospice Clinical Governance Strategy
13. Staff Handbook
14. Volunteer Handbook

## 4. Procedure(s)

### 4.1 : What is confidential information?

- 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, 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.

**Some examples of a breach of confidentiality include:**

- Mentioning to a friend or relative that you saw a mutual friend waiting for an out-patient appointment
- Using Hospice systems to check patient details when you are not involved in that person's care and have no legitimate right to do so.
- Mentioning to anyone out with a work context that you have seen a referral for a particular patient.

### 4.2 : Acting on the duty of confidentiality

- Patients are informed of their rights in relation to how the hospice handles confidential information through a leaflet “Confidentiality and your Health Record” (see appendix 5) available at Hospice and via Health Professionals and the issue is covered in the Hospice information booklet for patients and families.
- 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.

### 4.3 : 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 Line Manager and Caldicott Guardian.

## 6. References / Associated Standards / Guidelines

1. Access to Health Records Act 1990
2. Computer Misuse Act 1990
3. Copyright, Design and Patients Act 1988

4. Data Protection Act 1998
5. Freedom of Information (Scotland) Act 2002
6. Human Rights Act 2000
7. NHSiS ITSecurity Manual
8. NHSScotland Caldicott Guardian's Principles into Practice 201O
9. NHSScotland Code of Practice: Protecting Patient Confidentiality 2012
10. Privacy and Electronic Communication Regulations 2003
11. Public Records Scotland Act 2011
12. Regulation of Investigatory Powers Act 2000
13. Scottish Government Records Management: NHS Code of Practice (Scotland)
14. Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
15. December 2016 Introduction of new FOI tool ( voluntary sector)

## 7. Appendices

1 Confidentiality Guidelines Kilbryde Hospice
2 Caldicott: legal & professional requirements
3 Third party enquiries and disclosures
4 Information for patients on the use of their information
5 Confidentiality and your Health Records: Information for patients and carers leaflet (Kilbryde Hospice)

Appendix 1

**Kilbryde Hospice - Confidentiality Guidelines**

**Introduction**

1. Everyone working for or with the Hospice who records, handles, stores or otherwise comes across information that is capable of identifying an individual patient, has a personal duty of confidence to that individual and to his/her employer.
2. 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, amongst others.
3. 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**

4. 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.
5. 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**

6. Inadvertent or inappropriate disclosure of confidential information is potentially a serious matter. Adherence to the following principles will reduce the risk of this occurring.
7. If you are uncertain whether information is confidential or not, assume that it is.
8. Whenever possible, remove person-identifying details (e.g. name and address) and use other information such as the CHI number or Crosscare number.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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
14. 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.

15. Be particularly careful if work is taken home: the Hospice is still responsible for the data and it must be kept secure at all times. Patient records may not be taken home without permission from the Clinical Services Manager or Caldicott Guardian.
16. E-mail systems are inherently insecure: do not send confidential information by e- mail unless absolutely necessary and only if encrypted. See the Hospice's *Information Protection Policy and Guidelines* for further information.
17. Confidential papers must be securely packaged if they are to be transported or sent to another location. The Hospice's *Information Protection Policy and Guidelines* has further information transferring confidential information by post.
18. Always dispose of confidential material by the proper means. Papers must be put in designated confidential waste bags or bins, and send for shredding. To dispose of information stored on computer disks, call Roswell IT on 01355 593500 for advice.

**Relatives and friends**

19. 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.
20. 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**
21. 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**

22. 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.
23. 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 organisation. 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.

24. 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

25. 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.
It may well be good practice to ask for a Warrant before confidential information is released.

26. 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.

27. Theft, fraud and burglary (unless aggravated by assault) are unlikely to outweigh the duty of confidentiality to the patient. Information should not be disclosed in these cases. Seek guidance from the Caldicott Guardian if in doubt.

## 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.

## Consent for the use of information

28. Consent for the use of personal information is not the same as consent for carrying out clinical procedures, although it is often associated with a healthcare episode.

29. Implied consent for the use of identifiable information is no longer necessarily sufficient. It is acknowledged that it is not possible for explicit consent to be obtained for the use of data in all circumstances, although this is preferred.

30. Instead, patients are expected to give *informed* consent. Informed consent means that the patient makes a decision having been given sufficient information explaining the uses to which information (about them) may be put, and their rights with respect to the use personal information about them. The Hospice requires that all patients are given a copy of the leaflet Information for Patients, which contains a section on the use of information.

31. In normal circumstances, patients have the right to object to the use of their personal health data for purposes other than their immediate care. If consent is withheld, the possible consequences for the care of the individual must be clearly explained, but their decision must be respected unless circumstances are exceptional, for example as described about under Disclosures in the public interest, and Disclosures to the Police.

32. The reasons for any refusal of consent must be documented in the patient's notes.

33. Where a patient is not competent to consent, decisions regarding the use of that information must be made in the patient's best interests by those responsible for providing care, if necessary seeking the advice of the relevant senior clinician.

## Subject access

34. People are entitled, under the Data Protection Act 1998, to see information about themselves and to have copies of it if they wish (a Subject Access Request). There are some restrictions to the release of information.

35. All Subject Access queries should be directed to the Clinical Services Manager. There may be a charge for this service.

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

37. 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

38. 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 an incident form and report it.

39. 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.

## Further information

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

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

42. Kilbryde Hospice Information Protection Policy and Guidelines

43 Adults with Incapacity Act (2000)

## Appendix 2: 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 Margaret Mary Cowan.

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. |

### The Data Protection Act 1998

The Data Protection Act 1998 came into force in March 2000. Its purpose is to protect the right of the individual to privacy with respect to the processing of personal data. The Act laid down eight data protection principles:

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
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.
8. Personal data shall not be transferred to a country outside the European Union, 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

.

**The Human Rights Act**

As an employee of a public authority you have a duty to comply with Article 8 of the Human Rights Act 1998. This states that everyone has the right to respect for his/her private and family life, home and correspondence. There should be no interference with this right unless necessary in the interests of protecting public health and safety or preventing crime

**1990 Computer Misuse Act**

The 1990 Computer Misuse Act makes it a criminal offence to gain or attempt to gain unauthorised access to any program or data held in any computer. The more serious offences under the Act are:

- gaining, facilitating or attempting to gain unauthorised access to any program or data held in any computer, with the intent to commit further offences under the Act;
- carrying out any unauthorised action which is intended to modify the contents of any computer.

Anyone who tries to access a computer or system, or information thereon, to which they do not have authorised access rights is committing an offence. Modifying or attempting to modify information or programs is also an offence, and this would include introducing a virus into a computer or system.

## Appendix 3: Third Party enquiries and disclosures

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

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, 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 4: Information for patients on the use of their information

(The following is available as an information leaflet for patients.)

### Your information and how we use it

### Your personal health information

1. Every time you come into the hospice, information about you, your medical treatment and family background may be recorded, on paper and computer, to help us provide you with healthcare services. The information forms part of your Health Record and will be kept in case we need to see you again.
2. Members of the Hospice team looking after you may share your personal health information with each other. This team may include nurses, doctors, therapists, pharmacists and administrators plus students and trainees in medicine or other healthcare professionals who are looking after you.
3. Please note ALL staff working and training in Kilbryde Hospice are bound by law and a strict code of confidentiality and are regulated and monitored by the Hospice's Caldicott Guardian a role responsible for ensuring patients' rights to confidentiality are respected).

### How your records are used to help you

4. The staff involved in your treatment need to have accurate and up-to-date information to assess your health and provide you with care.
5. A record of any treatment or care you receive in hospital will be kept in case you return for further treatment and to assist other Kilbryde Hospice staff who treat you in the future both in the hospital and elsewhere.
6. Your records allow hospital staff to assess and investigate the type and quality of care you have received should the need arise.

### How your information can help Kilbryde Hospice

- to enable us to review the care provided for you and other patients, to ensure it is of the highest quality, make sure our services can meet all patients' needs in future and enable the production of Scottish Hospices statistics;
- to train healthcare professionals and support hospital research and development;
- to enable the hospital to be paid for your treatment and to support audits of Kilbryde Hospice services and accounts;
- to support the investigation of any incidents or issues that arise.

7. In addition, information may be used for research projects that have been approved by the Local Research Ethics Committee. You will be asked for your consent if we need to use any information that clearly identifies you. For instance, some research studies identify people so that information from the research can contribute to their future care.

### Sharing your information

8. Sometimes the Hospice is required to pass on information by law, for example:
   - when an infectious disease is encountered that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
   - where a formal court order has been issued.

9. You may receive care from non-NHS staff (for example Social Services), with whom it is necessary to share information about you to enable them to work with medical staff in providing your care. Your information will only be made available if there is a genuine need for it and where your consent is needed we will contact you for permission.
10. The principal NHS partner organisations with which information may be shared are NHS Lanarkshire, GP practices and Ambulance services. If it is necessary to pass on information about you, personal details are removed whenever possible.

**Your information rights**

11. You have the right to know how we will use your personal information.
12. You have the right of access to your Health Record (your medical notes). This is known as “Right of Subject Access”.
13. You have the right to object to us making use of your information.
14. 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.
15. 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 Subject Access Request**

16. 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.
17. 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.
18. 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 Subject Access Request, to the Chief Executive Officer

Margaret Mary
Cowan
Caldicott Guardian
Kilbryde Hospice

## CONFIDENTIALITY

## AND YOUR HEALTH RECORDS

**Information for patients and carers**

### Confidentiality

- Kilbryde Hospice must keep your personal health information confidential. It is your right.
- Your personal health information is kept in records. Your health records contain information about your health and any care or treatment you have received. Records can be written on paper, held on computer, or both.
- Kilbryde Hospice staff use your information to give you the care and treatment you need. They add to your health records every time you get care or treatment.
- Your information may be shared with other Kilbryde Hospice staff involved in your care.
- Sometimes Kilbryde Hospice uses relevant information about your health to help improve the general public's health and NHS services or to check that money has been spent properly. Wherever possible, information that identifies you is removed.
- If Kilbryde Hospice uses information which identifies you for teaching and research, they must ask your permission.
- Sometimes information will be shared with people outside Kilbryde Hospice, for example, with a social worker, but only if you agree.
- Usually Kilbryde Hospice will not share your personal health information with people such as a relative, carer or friend without your permission.
- Sometimes the law allows Kilbryde Hospice to share your information without your permission, for example to investigate a serious crime or to protect a child.
- If you are concerned about your information being shared, you can object. You should tell a member of Kilbryde Hospice staff providing your care.

### How to see your health records

- You have the right to see or have a copy of your health records.
- If you want to see or get a copy of your health records, you should write to the Clinical Services Manager

Kilbryde Hospice
McGuinness Way
East Kilbride G75 8GJ
01355 20 20 20

- You do not need to give a reason for wanting to see your records but you may be charged a fee.
- If you are not happy with anything written in your records, you should speak to a member of staff providing your care.

**Under the Data Protection Act 1998, you have a right to know who holds personal information about you. For the Kilbryde Hospice please write to the**

Kilbryde Hospice
McGuinness Way
East Kilbride G75 8GJ
01355 20 20 20

**For more information**

- The leaflets produced by the Hospice "Confidentiality – it's your right" and "How to see your Health Records" give you more information about your right to confidentiality and your right to see your health records.
- Further information can be found at www.nhsis.co.uk/confidentiality.

## Suggestions and Comments

Our Team at The Kilbryde Hospice is committed to providing a quality service. Your views on our care and support are important and can help us achieve continuous improvement and development. If you have any suggestions about how the Hospice services can be improved, there is a suggestion box on the desk of the ground floor reception area. Confidentiality will be maintained and the box is emptied weekly. All suggestions will receive a written reply within 10 working days.

## Complaints

Any complaints will be handled with the utmost confidentiality and will be acknowledged in writing within two working days. If you have any complaints please speak to the nurse in charge. If your complaint cannot be resolved immediately it will be passed to a senior member of the management team.

All patients, carers and visitors have the option of discussing concerns with:

**Clinical Services Manager, Tel: 01355 20 20 20**
Or write directly to
**Chief Executive Officer**
**Kilbryde Hospice**
**McGuinness Way**
**East Kilbride G75 8GJ**

**info@kilbrydehospice.org.uk**

The clear aim is to resolve all complaints within 28 working days and to provide you with a full explanation of the outcome. Should you feel that your complaint has not been resolved satisfactorily by the Hospice, you may contact the Healthcare Improvement Scotland Office directly at any stage.

**Healthcare Improvement Scotland**
**Gyle Square**
**South Gyle Crescent**
**Edinburgh**

**EH2 9EB**

**Tel: 0131 623 4319**

**www.healthcareimprovmentscotland.org**

**Appendix 5:**

# DATA PROTECTION ACT 1998

## *SUBJECT ACCESS REQUESTS*[1]

Kilbryde Hospice's Information Requests Compliance Policy 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.

The Data Protection Act 1998 (the DPA) 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 subject access request.

The Hospice's Confidentiality Policy states that all individuals have the right to request access to personal 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 DPA.

We will only apply the exemptions that allow us to refuse a request to access by an individual to his or her personal data when there is a clear and justifiable reason for doing so. The Appendix lists **some** of the DPA exemptions.

The rights of people to access their personal information is set out in section 7 of the DPA. This section gives people the right to "access" their personal data. People are able to ask that they

1) are informed by Kilbryde Hospice whether it processes (i.e. has/uses) any personal data in relation to them
2) if personal data is held by Kilbryde Hospice l, be given a description of

[1] This guide uses standard words and phrases that are either set down in or are commonly used in connection with data protection. You should read these words and phrases as explained in the Glossary of Terms that is available on the Council's intranet.

a) the information
b) the purposes for which Kilbryde Hospice is using or will use the information and
c) details of to whom the data is or may be disclosed and

3) to get, in an understandable way:
a) a copy of the personal information and
b) details of the source of the personal data (i.e. the person or body that gave the information to Kilbryde Hospice).

In the past, we have viewed these rights as being separate. So, if an individual requested a copy of his personal data, we would deal with the request on the basis that this was all he was entitled to. However, a request under any of the provisions includes a request under all of the others.

If we send out a copy of all of the requested personal information, we will probably satisfy the applicant. However, sending out a copy will not explain

- the purpose for which the information is held/used/processed (where this is unclear),
- the recipients or
- the sources from whom Kilbryde Hospice obtained the personal data (where this did not come from the applicant)

to the applicant.

Accordingly, when we are processing a request, we must remember that

- the data subject has the right to obtain additional information about the use of the personal data in question and
- we must provide this information if requested to do so, unless an exemption in the DPA applies to that information.

However, the purpose of the subject access rights is to allow the data subject to be able to exercise their other rights under the DPA and for no other purpose. There have been court decisions to say that it is not appropriate to use the subject access rights to obtain information that is intended to be used for another purpose. However, we cannot ask the requestor about his or her motive behind making the request. Consequently, a subject access request should only be refused if it is clearly for a different purpose – such as obtaining information for a court action against Kilbryde Hospice or someone else etc and this different purpose has been explained by the data subject.

If you believe that you are dealing with a request for information that is not a subject access request because it is for another purpose, you must contact and discuss whether this should happen with your manager before refusing the request.

Please note that a subject access request is different from data sharing with someone. Data sharing is where Kilbryde Hospice is sharing information (possibly including personal data of other people) with someone in connection with the Hospice's functions or because it has the consent of the data subject to do so or another justifiable reason which is compliant with the requirements of the DPA.

In those cases, Kilbryde Hospice has usually discretion as to whether to share the information and its considerations on whether to do so would not follow this guidance. Data sharing must be done in compliance with Kilbryde Hospice Information Governance

## Appendix

## Exemptions under the Data Protection Act 1998

If Kilbryde Hospice receives a request from a person to get their own personal data there are some circumstances when we do not need to comply with the request.

We can refuse to comply with a request i.e. not process it at all because while it is the applicant's personal data, the DPA rights of access do not cover it. These situations are

- the purpose of the request is different from that intended by the DPA
- if, in answering the request, we have to give another person's personal data and
    - no consent has been obtained and
    - under all of the circumstances, it is unreasonable to comply without consent
- if it is impossible to supply the personal information in a permanent form or it would involve a disproportionate effort
- if the applicant agrees that some of the data need not be supplied to him/her
- if the applicant has made an identical or similar request before and there has not been a reasonable interval between the requests
- if the information is in paper documents which are not held on a file or similar that is part of a structured filing system using a reference to the individual (or criteria relating to individuals), the cost incurred by Kilbryde Hospice (calculated in terms of the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004) in complying with the request exceeds the prescribed limit (£450 – calculated at £25 per hour of employee time).

However, if these exemptions do not apply, we must deal with the request. This does not mean that we must give the information out. The DPA contains some exemptions from the disclosure provisions.

The exemptions under the DPA are class or harm based. A "class" exemption applies where the personal data falls within a specific type that we should not give out. A "harm" exemption applies where the personal data could prejudice something that Kilbryde Hospice or someone else does.

**Examples of Class based exemptions are**

- Where the personal information is publicly available i.e. in a statutory public register
- References given (or to be given) **by** Kilbryde Hospice in confidence for the purposes of education, training or employment of the applicant (Note this does not apply to references given Kilbryde Hospice)
- Examination scripts
- Personal data where confidentiality of communications could be maintained in legal proceedings

**Examples of "harm" based exemptions are**

- Where disclosure of the personal data would be likely to prejudice
    - prevention or detection of crime
    - the apprehension or prosecution of offenders or
    - the assessment or collection of any tax or duty or imposition of a similar nature
- Where disclosure of the personal data would be likely to prejudice the proper discharge of regulatory functions in respect of
    - securing health, safety of persons at work, or
    - protecting persons other than persons at work against risk to health and safety arising out of or in connection with the actions of people at work
- Where disclosure of the personal data would be likely to prejudice management forecasting or management planning to assist Kilbryde Hospice in the conduct of any business or other activity
- Where disclosure of the personal data would be likely to prejudice negotiations with that person

**Appendix 6 :**

*Information Request Pack*

Dear

**Data Protection Act 1998 (DPA)**
**Data subject 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.

**Charging**

Kilbryde Hospices charges for processing requests under the DPA. This is a set fee of £10 unless waived by the Hospice.. The request form contains details about how to pay this fee and when the fee is waived by the Hospice.

**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 not be able 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 DPA 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,