

CONFIDENTIALITY POLICY & GUIDELINES

1.0 INTRODUCTION

1.1 Confidential Information – What is it?

DRH aims to assist service users to meet their basic human needs. Maintaining confidentiality is one way we can acknowledge the following innate and universal needs:

- The need for security
- The need for a sense of autonomy and control
- The need for privacy

A duty of confidence arises when one person discloses information to another (e.g. service user to nursing/support worker) in circumstances where it is reasonable to expect that the information will be held in confidence.

Information should be considered confidential if it can be related in any way to a specific individual. The main areas of concern are about patient and staff records and include any information that has not been fully anonymised.

Confidential information will be found in a variety of formats including paper, computerised (including portable devices such as laptops and memory “sticks”), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone (including mobiles) and general conversation.

1.2 Data Protection 1998

The Data Protection Act 1998 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature. It is founded on the following set of eight good practice principles:

Principle 1 – Personal data shall be processed fairly and lawfully and in particular shall not be processed unless specified conditions can be met.

Principle 2 – 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 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 adequate and where necessary kept up to date.

Principle 5 – Personal data processed for any purpose or purposes shall not be kept any 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.

Principle 7 – Appropriate technical and organizational measures shall be taken against unauthorized 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 any 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.

2.0 SERVICE USERS PERSONAL INFORMATION

This guidance is based on the following principles:

- 1. Service users are entitled to expect that information about them will be treated as confidential and that staff will refrain from voluntary disclosure of any personal information, learned directly or indirectly, to an unauthorised third party.**
- 2. The importance of making service users fully aware that DRH staff and sometimes staff of other agencies, involved in their care, need to have strictly controlled access to such information, anonymised wherever possible.**

It is in everyone's interests that DRH functions efficiently and effectively and makes the best use of available resources. To this end personal information about service users is not only essential for the prime task of delivering appropriate support and care. It is also necessary for a number of other purposes:

- Assuring and improving the quality of care and treatment in the context of effective team-working.
- Protecting public health

- Coordinating care with that of other agencies, i.e. local authority, social services, voluntary and independent services.
- Effective administration which includes:
 - Managing and planning services
 - Auditing Care
 - Auditing Accounts
 - Payment of Staff
 - Risk management and health and safety
 - Investigating complaints and potential legal claims.
- Training
- Statistical information

As a consequence, service users information will be seen and used by a number of DRH professional and administrative staff, as well as staff of other agencies who may be purchasing care or contributing to the care of service users. Service users would be unlikely to trust staff with detailed information if they thought this might be passed on to others without proper controls. It is therefore central to this policy that DRH staff are under a legal duty to keep records confidential. In addition the guidance makes clear that personal information should be anonymised wherever possible.(e.g. using initials or date of birth rather than full name)

3.0 Responsibilities

Every member of staff (including agency, bank, volunteers, and student placements) will at some time in the course of their work, have to handle and/or be privy to confidential personal information whether relating to staff, service users or their carers, family or friends or any other individuals connected to DRH in some way.

Staff need to be aware that:

- They are individually responsible for the safekeeping of that information on behalf of DRH , when it is in their possession.
- Everyone working for DRH who records, handles, stores or comes across information that could identify a service user has a Common Law Duty of Confidence to that service user and to DRH.
- Serious breaches of this policy may lead to disciplinary action, including dismissal
- Professional obligations of confidentiality must be applied (e.g. NMC; GSCCoFC).

4.0 STAFF PERSONNEL INFORMATION

- 1. Staff information must be kept in secure cabinets – this includes supervision records**
- 2. Access to information concerning staff is on a *need to know basis* to which only nominated managerial, administrative and financial staff have access. Permission to receive information from personnel files and payroll other than nominated staff must first be obtained from the person in charge of those records.**

DRH expects that all staff will demonstrate respect and courtesy for others in their general conversation. This expectation would preclude careless or malicious gossip and overt criticism of others. It does not preclude discussion of performance of staff in the appropriate setting or the use of the grievance procedure.

Any requests by a third party for staff personal information, e.g. details of salary for mortgage purposes, etc. must be authorised in writing by the member of staff concerned before the information is released. Salaries should not be discussed over the telephone unless it is ascertained prior to the discussion that the person inquiring is the member of staff concerned. Queries for details of pensions and other personal details should be placed in writing prior to any information being divulged over the telephone. This is to ensure that staff are confident that their personal information is secure.

Personnel and payroll files will be kept for 6 years after the person leaves or until their 70th birthday whichever is the later and will then be shredded.

Files on unsuccessful applicants for posts will be kept in a secure file for six months and then shredded.

5.0 NATIONAL MINIMUM CARE STANDARDS

DRH endorse the National Care Standards:

- Staff should treat information given to them by service users in confidence and should handle all information about them in accordance with DRH Policy, with the Data Protection Act 1998 and in the best interests of the Service user.
- That service users have access to the Policy and Procedures on confidentiality and that they understand how breaches of confidentiality are dealt with by DRH
- Service users individual records are accurate, secure and confidential.
- Staff know when information given to them in confidence must be shared with their manager or others.

- That any agencies providing services to the service user understand the principles governing the sharing of information.
- Information given in confidence should not be shared with families, friends or carers against the service users wishes.

6.0 BASIC PRINCIPLES

Generally, whenever a service user tells a member of staff anything, unless they make it explicit that the information can be freely shared, the information exchange is based upon the assumption that it is private and should not be passed on to anyone other than those who "need to know" in order to provide consistent and informed support. Such information can be classified as "confidential" and implies a duty of confidentiality on staff. This not only applies to information given by a service user, but also to third party information and information kept on file. All staff have an obligation to respect the confidential nature of such information and this obligation prohibits them from disclosing information about service users to other interested parties without the consent of the service user.

Personal information held on a computer system is safeguarded by the Data Protection Act 1988. This places obligations on those who record or use information, while at the same time giving specified rights to people about whom information is held. Further information on the Data Protection Act can be found at Appendix A, Policy No.44 The Management of Records and Information

6.1 When is consent required?

Explicit or Express Consent ***need not*** be obtained when:

A service has provided confidential information for the purpose of receiving care and support and, who has been made fully aware (as far as is practicable) of who will need to see information about them in order to provide care and support. Their consent to their information being used in this way can be termed "implied".

Explicit or Express Consent ***must*** be obtained when:

The purpose/use of information changes or could include disclosure outside that deemed as "Care & Support Purposes". For example, consent must be obtained prior to disclosure to or use for research, teaching (excluding local audit/assurance of quality of care provided), government departments, police & law courts. Consent where possible should be in writing.

In those circumstances where a service user is unable to give informed consent consultation should take place with a close family member before disclosure takes place.

Service User Choice

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

Service users have a right to change their mind about giving, withholding or withdrawing consent at any time. Full explanation must be given to the service user in cases where the withdrawing of consent may not always be possible (i.e publications –where an article written with prior consent has already been published).

Generally, information about service users employed for educational purposes (teaching, publications) can be easily anonymised.

7.0 OTHER PERSONAL INFORMATION

Personal information concerning staff or service users is also collected. An obvious example is personal addresses or financial information. Details of ethnic origin may also be collected. All such information is held in strict confidence and must be treated in the same way as personal health information.

8.0 REQUESTS FOR INFORMATION

Staff will not normally provide information to relatives, spouses, friends or advocates without the consent of the individual concerned. However, many service users do not have capacity to give or withhold explicit consent. In certain circumstances consent to disclosure may be implied. For example, close family members who have consistently taken an interest in the welfare of a relative in the care of DRH can reasonably expect to be regularly briefed on that person's well-being. However, if a service user explicitly states that they do not wish confidential information to be shared with members of their family then that choice must be respected.

Staff can be asked for reports by insurance companies, solicitors, employers, etc. Reports should not be provided without the written consent of the person concerned or (when the service user lacks capacity) their recognised advocate (which may be a family member) and the Chief Executive or Deputy Chief Executive informed of the request.

Any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. There are certain circumstances when information can be passed on:

- 1. The recipient needs the information because he or she is or may be concerned with the service users care and treatment or that of another service users whose health may be affected by the condition of the original service user**
- 2. Information is required by court order**
- 3. Information is required by statute**
- 4. Information is required in the public interest**

NOTE *For items 2 – 3 and 4 – The Chief Executive or Deputy Chief Executive must be informed before the requested information is released.*

8.1 Court Orders

A court order requiring disclosure of health information should specify clearly what information is required to be provided, by whom to whom, etc. The Chief Executive or Deputy Chief Executive will seek legal advice if the order is unclear. The Home Manager responsible for the service users care will be consulted about the disclosure, in case there is a risk that it may harm the health of the service user or other person(s) If there is such a risk, legal advice will be sought urgently on the possibility of seeking an amendment to the order.

8.2 Statutory Disclosures

In certain circumstances DRH may be required by law to pass on what would otherwise be confidential information. Examples of disclosures required by statute are as follows:

Notification of Communicable Diseases

Public Health Act 1936

Public Health (Infectious Diseases) Regulations 1988(SI 1988 No.1546

Public Health (Control of Disease)Act 1984

Notifications of Poisonings and other serious accidents at work

Health & Safety at Work Act 1974

Reporting of Injuries, diseases and dangerous occurrences

Notifications of Abortions

Abortion Act 1967 Section 2

Abortion Regulations 1991 (SI 1991 No 499)

Notification of Drug Addicts

Misuse of Drugs Act 1971 Section 10

Misuse of Drugs (Notification of and supply of addicts) Reg. 1973(SI1973 No799)

8.3 Disclosures in the Public Interest

The main public interest justifications for disclosure of health information include:

- For monitoring purposes (e.g. collation of statistics)
- Serious risk to the health of other individuals, such as the reporting of adverse drug reactions and of investigation and control of communicable disease
- Serious risk to public health such as exchanges of information on a "need to know" basis within legal constraints and the reporting of notifiable disease.
- The prevention, detection or prosecution of serious crime - however, the crime must be sufficiently serious for the *public interest in disclosure* to prevail over the *public interest in confidentiality*. Also it must be established that without the disclosure, the task of preventing or detecting the crime would be seriously prejudiced or delayed. Satisfactory undertakings must be obtained that the personal health information disclosed will not be used for any other purpose and will be destroyed if the suspect is not prosecuted or is discharged or acquitted.

There is no absolute definition of serious crime, but could include:

- Serious harm to the security of the state or to public order
- Serious interference with the administration of justice or with the investigation of an offence.
- Death or serious injury
- Substantial financial gain or serious loss

These definitions include such crimes as murder, manslaughter, rape, and kidnapping. This list should not be treated as either conclusive or exhaustive but used as a guide.

8.4 Disclosures to Statutory Regulatory Bodies

Service users or staff records and information may be required to be disclosed to Statutory Regulatory Bodies such as the CSCI, Healthcare Commission or professional regulatory bodies. This could be for investigation into a complaint of abuse or into a health professionals fitness to practice. Wherever practicable the need to disclose should be discussed with the person involved and permission for disclosure obtained. There may be exceptional cases where, even though the service user or staff object, that disclosure is justified.

8.5 Disclosures for Educational Purposes

Disclosures of health information for teaching purposes should be regarded as disclosures for a DRH purpose. Wherever possible, service user details should be anonymised.

9.0 INFORMATION ABOUT ETHNIC ORIGIN OR RELIGIOUS AFFILIATION

When service users are admitted to DRH Homes, the religious persuasion of the Service user should be recorded if they are willing. This information may not be passed to any religious organisation or its members outside DRH without the service users consent. The ethnic origin of service user and staff may be recorded for monitoring purposes.

10.0 INFORMATION TO THE MEDIA

Maintenance of positive relations with the press, TV and radio is important. The media fulfil an important role in reporting on the activities of public bodies, charities and companies and a relationship of understanding and trust should be encouraged. DRH wish to respond positively to inquiries and to avoid misunderstandings. Only the Chairman, Chief Executive or Deputy Chief Executive are authorised to speak for DRH and all inquiries should be directed through Head Office.

The Chairman, Chief Executive or Deputy Chief Executive will not disclose personal information to the media, or any other unauthorised person without the service users consent to such disclosure.

11.0 INFORMATION FOR FUND-RAISING ACTIVITIES

The use or disclosure of personal information for the purpose of fund-raising activities can be justified only when the service user has given express consent to such disclosure.

12.0 UNAUTHORISED DISCLOSURE OF INFORMATION

Any disclosure in circumstances other than those provided for in this policy is likely to constitute a breach of confidentiality and may be regarded as an unauthorised disclosure.

Unauthorised disclosure of personal information is a most serious matter, which will almost always warrant disciplinary action, including dismissal.

Those working for DRH must be on their guard against people who seek personal information by deception – for example – a person posing as a doctor, nurse, social worker or relative. If a member of staff is asked to

provide personal information by a person not known to him, he must verify that the person has a right to the information before releasing it.

Any contractors working within DRH are under strict legal obligations requiring them to guard and use confidential information no less securely than DRH staff. An outside contractor who breaches confidentiality will be liable to appropriate action.

Reviewed April 2003

Reviewed September 2004

Reviewed & amended April 2008

Next review due April 2011