Data Protection and Confidentiality Policy

November 2013
Title: Data Protection & Confidentiality Policy

Reference Number: Corp11/003

Original Implementation Date: June 2011

Reviewed: November 2013

Next Review Date: November 2015

Responsible Officer: Assistant Director of Performance & Service Improvement
# Table of Contents

1. Introduction  
2. Statement of Policy  
3. Data Protection principles  
4. Disclosure of Personal Information  
5. Handling of Personal Information  
6. Compliance  
7. Third Party Users of Personal Information  
8. Staff Responsibilities  
9. Policy Awareness  

Equality Statement  

**Appendix 1** Guidance for Directors, Managers and Staff  
- Management Responsibilities  
- General Responsibilities  
- Holding and passing on patient or client information  

**Appendix 2** Relevant Legislation  
**Appendix 3** Guidance Notes  
**Appendix 4** Trust Patient and Client Information Systems Data Protection Protocol  
**Appendix 5** Confidentiality – Trust General Code of Practice  
**Appendix 6** Principles Governing Information Sharing
1. Introduction

The Western Health and Social Care Trust is fully committed to complying with the Data Protection Act 1998 (DPA) which came into force on 1 March 2000. This policy sets out responsibilities and provides a set of principles covering all aspects of processing personal information. (see Appendix 3 for definition of ‘processing’)

The term ‘personal information’ refers to information relating to any identifiable individual and it is important to be aware that health and social care information is considered in the DPA to be “sensitive information” requiring the highest levels of care and protection. The ease with which personal information can be passed within Health and Social Care (HSC) - often electronically - is an undoubted benefit for patients and clients and for those involved in their care and treatment. However, all those concerned need to be aware of their legal responsibilities under the Act to protect the confidentiality of patient and client information.

Personal information on staff is also protected by the DPA. The Act affords staff the same rights of protection for, and of access to, their personal information held by the Trust. While this document concentrates on information held on behalf of patients and clients, the principles are generally applicable to staff information.

Everyone working for or within the Trust who records, handles, stores or otherwise comes across information, has a statutory duty under the DPA, along with a duty of confidentiality in common law, to patients and clients, and to the Trust as an employer. These duties apply equally to students or trainees, or to staff on temporary placements. Non-HSC staff working in, or for, the Trust are subject to the same duties of confidence. Clinical, social care, and management staff also have a duty to support the standards of confidentiality set by their professional bodies.

The Trust will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the Act.

2. Statement of Policy

We need to collect and use personal information about people in order to provide our services and carry out our business. These may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, we may be required by law to collect and use information. It is the Trust policy that all personal information, whether in paper, electronic or any other format, must be handled in strict confidence and managed in accordance with DPA and associated legislation and guidance (see Appendix 2).
3. Data Protection Principles

The data protection principles contained in this policy, apply equally to all Information and Communication Technology (ICT) security policies and procedures involving the use and transfer of personal information.

The Trust fully supports and complies with the eight principles of the Data Protection Act. In summary, this means personal information must be:

(i) processed fairly and lawfully;
(ii) processed for limited purposes and in an appropriate way;
(iii) adequate, relevant and sufficient for the purpose;
(iv) accurate and up-to-date;
(v) kept for as long as is necessary and no longer;
(vi) processed in line with individuals’ rights (see Appendix 3);
(vii) secure and protected against unlawful access, loss or damage
(viii) only transferred to other countries that have suitable data protection controls.

Our purpose for holding personal information, along with a general description of the categories of people and organisations to which we may disclose it, are listed in the Information Commissioner’s Data Protection Register. Details can be found on the Information Commissioner’s Office (ICO) website at www.ico.gov.uk.

4. Disclosure of Personal Information

Strict conditions apply to the disclosure of personal information both internally and externally. We will not disclose personal information to any third party unless we believe it is lawful to do so. Respect to confidentiality will be given where appropriate.

The Trust will seek the consent of patients and clients before passing personal identifiable information on for any reason other than to fulfil the justifiable purposes laid down in the Caldicott report 2013 (See Appendix 1 – Section 3 – Guidance for Directors, Managers and staff).

The Trust will seek the consent of staff for the passing on of identifiable personal information for any purpose other than those outlined to staff on appointment. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:
• we have the statutory power or are required by law to do so; or
• the information is clearly not intrusive in nature; or
• the member of staff has consented to the disclosure; or
• the information is in a form that does not identify individual employees.

The Trust is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud. The information shared is usually personal information which will be used for carrying out data matching exercises. Further information is available from the Trust website on the ‘National Fraud Initiative’ fair processing notice (www.westerntrust.hscni.net).

5. Handling of Personal Information

The Trust handles all identifiable information securely and in keeping with the requirements of the DPA and other associated legislation (see Appendix 2).

All staff will, through appropriate training and responsible management:

• fully observe conditions regarding the fair collection and use of personal information;
• meet our legal obligations to specify the purposes for which personal information is gathered and used;
• collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
• ensure the quality of personal information used;
• apply strict checks to determine the length of time personal information is held;
• ensure that the rights of people about whom information is held can be fully exercised under the Act (see Appendix 3);
• take appropriate technical and organisational security measures to safeguard personal information;
• ensure that personal information is not transferred abroad without adequate safeguards.

The Trust takes disciplinary action against any and all members of staff found to have breached patient/client confidentiality and ensures that staff are aware that they risk personal prosecution for breaches of the DPA.
6. Compliance

The Trust will ensure that:

- there is always someone with specific responsibility for Data Protection in the organisation;
- patients and clients are pro-actively informed of the uses to which their information is put. It will also inform staff, on appointment, of the uses to which their personal information is put, e.g. equal opportunity monitoring.
- consent is sought before passing personal identifiable information on for any reason other than to fulfil justifiable purposes;
- all Subject Access Requests (SARs) will be dealt with in accordance with the Data Protection Act and within the 40 day time limit;
- staff are reminded of their obligations under DPA;
- everyone managing and handling personal information understands that they are directly and personally responsible for following good Data Protection practice;
- only staff who need access to personal information as part of their duties are authorised to do so. Unauthorised access to personal information, either in paper or electronic format, is considered to be a breach of DPA and the Trust policy.
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- consent is sought before taking identifiable photographic, video, or audio recordings, where possible. If this is not possible, such images are not used without the consent of the patient/client, or approval of the appropriate Data Guardian.
- CCTV systems are used and managed in accordance with the Information Commissioners ‘CCTV data protection code of practice’ (see Appendix 1 - section 2.12)
• Information and Communication Technology (ICT) security policies and procedures are in place to manage the storage, use and transfer of personal information and that these policies/procedures are regularly reviewed.

• approved 'retention and disposal' guidelines are followed for all personal information and arrangements are in place for the secure disposal of records when they are no longer needed.

• the way personal information is managed and handled will be regularly reviewed and evaluated;

To assist in achieving compliance, the Trust has:

• delegated responsibility to Directors, accountable to the Trust Board, to act as Personal Data Guardians who will have overall responsibility for Data Protection. The Medical Director and the Executive Director of Social Work fulfill this function.

• delegated responsibility to the Assistant Director, Performance and Service Improvement, for day-to-day management of data protection processes.

• appointed a Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO).

• appointed a Data Protection Officer responsible for monitoring compliance of the Act throughout the Trust, providing advice and guidance; dealing with escalated complaints from data subjects; liaising with the ICO and HSC solicitors on data protection issues;

• created a Data Protection Policy and associated procedures and protocols providing detailed guidance on data protection issues; and

• an awareness and training programme in place, to include induction training and regular refresher training, to ensure that staff at all levels are aware of their general and specific responsibilities under data protection legislation to protect patient and client confidentiality.

Further guidance is included in the attached Appendices to assist staff at all levels to uphold the policy principles.
7. Third Party Users of Personal Information

Any third parties who are users of personal information supplied by the Trust will be required to confirm and demonstrate that they will abide by the requirements of the Act. There will be an expectation that these parties will audit their compliance with the DPA and will provide assurances to the Trust in this respect.

8. Staff Responsibilities

All staff have a responsibility to protect the personal information held by the Trust. They will take steps to ensure that personal data is kept secure at all times and protected against unauthorised / unlawful or accidental loss, damage or disclosure. This applies to all personal identifiable information held in all formats, whether is it in patient, client or staff files or in any other format such as diaries, message books, notebooks, appointment books, emails and other notes held about individuals.

In particular staff will ensure that:

- they are appropriately trained in the handling of personal information;
- paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- where they are required to take personal information away from Trust premises as part of their work, including information held in all formats, this should be held securely at all times and everything possible done to safeguard against unauthorised access or accidental loss or damage.
- personal information is transferred securely at all times, whether it is being sent electronically or by post, either internal or external to the Trust.
- personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically;
- all Trust ICT security policies are adhered to when processing personal data to ensure adequate levels of protection are maintained. The ICT Policies should be read in conjunction with this policy.

Where staff, as part of their responsibilities, collect, hold and process information about other people, they must comply with the Trust policy and guidance. No one should disclose personal information outside this guidance or use personal data held about others for their own purposes.
RESPONSIBLE OFFICERS:

The Trust’s **Personal Data Guardians** are responsible for:

i. The development and review of Trust confidentiality policies and associated guidance, including this policy.

ii. Consideration of all requests for the transfer of identifiable information which do not fulfil the justifiable purposes drawn from the Caldicott Report and set out in Appendix 1 (Section 3 of Trust guidance).

iii. Advice and guidance on individual and Trust responsibilities contained within the DPA 1998 and other associated legislation.

iv. Advice on the use of CCTV footage, on non-consented audio and video recordings, and on data protection issues associated with research and audit studies.

v. Investigating any reported breaches of the DPA including requiring action to remove or minimise the risks of similar breaches.

**Directors** are responsible for ensuring the implementation of this policy within their respective directorates and for the regular monitoring of implementation processes to uphold the policy principles and meet the statutory requirements of the DPA and associated legislation. Directors are also responsible for ensuring that breaches of the DPA are reported via the appropriate governance channel, and to the Personal Data Guardians.

Some directors have specific responsibilities. For example, the Director of Human Resources (HR) or a delegated HR assistant director/manager is responsible for ensuring the inclusion of data protection and confidentiality information for new staff in ‘new start’ packs and for the inclusion of confidentiality clauses in contracts of employment, including honorary contracts. The Director of Performance and Service Improvement will also have a particular interest in respect of ICT security policies to ensure the proper protection of personal information held electronically.
The Assistant Director of Performance and Service Improvement has particular responsibility for the day-to-day management of data protection issues, including administration of access requests made under the DPA and the routine monitoring of DPA processes and procedures to ensure continuing compliance with the legislation and with Trust policy. He/she liaises closely with the Trust’s Data Guardians on data protection and confidentiality issues.

9. Policy Awareness

All new members of staff will be made aware of this policy through the induction programme and advised that it can be accessed on the intranet site or through their line manager. Existing staff and any relevant third parties will be advised of the policy which will also be posted on our Internet site, as will any subsequent revisions. All staff and relevant third parties must be familiar with and comply with this policy at all times.

EQUALITY AND HUMAN RIGHTS STATEMENT: The Western Health and Social Care Trust’s equality and human rights statutory obligations have been considered during the development of this policy.
Appendix 1

Guidance for Directors, Managers and Staff

INTRODUCTION: This guidance has been developed to assist staff at all levels to uphold the policy principles contained within the Western Health and Social Care Trust’s policy document on data protection and confidentiality. It should be read as an appendix to the policy.

This guidance is divided into 3 sections as follows:

Section 1: **Directors’, Assistant Directors’ and senior managers’ responsibilities:** This section highlights the duty of confidence owed to patients, clients and staff by the Western Health and Social Care Trust (the Trust) and by each individual member of staff. It provides information on specific areas of responsibility, and it highlights the application of the Data Protection Act 1998 to manual as well as computer held records, and the resulting implications. All directors, assistant directors and senior managers must be familiar with this section.

Section 2: **General responsibilities:** These responsibilities apply to all employees of the Trust. They include informing patients and clients of the uses to which their information is put, obtaining consent to passing on their information, securing patients’, clients’ and employees’ rights to access their personal information, and dealing with police and media enquiries. A number of Trust protocols for handling confidential information are highlighted in this section.

Section 3: **Holding and passing on patient and client information:** This section summarises the recommendations and principles from the Caldicott Report 2013 and outlines the Trust’s arrangements to secure these principles. All staff likely to be involved in passing on information for purposes other than those related to delivering social and health care and treatment must familiarise themselves with this section.
SECTION 1: MANAGEMENT RESPONSIBILITIES

1.1 Implementing the Policy: The Trust’s policy on ‘Data Protection and Confidentiality’ applies throughout all directorates and departments within the Trust, without exception. Responsibility for ensuring implementation of the policy within directorates lies with the director, who may delegate that responsibility to an appropriate assistant director/manager.

1.2 Informing patients and clients: It is the responsibility of the relevant director or delegated assistant director/manager to ensure that the Trust’s information leaflet ‘How we use the information you give us about yourself’ is freely available in all patient and client waiting areas and other suitable areas within the Trust and that every opportunity is taken to provide the leaflet to patients and clients or to include its contents in relevant publications. Additional copies are available from the office of the Head of Information and Records.

These leaflets supplement the advice provided on the back of all letters produced from the Patient Administration System including appointment and admission letters. It is particularly important that arrangements exist in each of the service user directorates to ensure that these leaflets are readily available to patients/clients making unplanned attendances/admissions, including patients attending A&E departments.

Arrangements must also be made by the Human Resources department to inform new staff, on appointment, of the uses to which their personal information is put, including information on the National Fraud Initiative.

1.3 Staff Awareness: To secure staff awareness of their data protection and confidentiality responsibilities, all contracts of employment with the Trust must contain a duty of confidentiality clause. In addition, all newly appointed staff must receive information about their responsibilities regarding the protection of personal information. Managers must ensure that all newly appointed staff attend the Trust’s corporate staff induction programme, which includes advice on the protection of patient/client information. A copy of this policy should be readily available for reference in all departments and wards.
SECTION 2: GENERAL RESPONSIBILITIES

The Trust’s ‘Data Protection and Confidentiality’ policy requires that all information on patients, clients and staff is treated in strict confidence and in compliance with legislative requirements and guidance provided in the Data Protection Act 1998 and associated legislation and guidance. The following information is provided to help all staff meet their responsibilities in respect of data protection. Further advice or guidance on these or on other issues associated with data protection or confidentiality is available from Trust Headquarters by contacting the Personal Data Guardians or the Assistant Director, Performance and Service Improvement.

It is important that staff are aware that the Trust will take disciplinary action against any and all members of staff found to have breached patient/client confidentiality. Staff should also be aware that they risk personal prosecution for breaches of the DPA, especially where they have failed to take account of the requirements of this policy.

2.1 Records and Record Keeping

- Personal information should be adequate, relevant and not excessive for the reason(s) for which it is collected or used.

- Personal information should be accurate and kept up to date.

- All records should be clear, relevant and concise, and indicate the identity of any persons who have made an entry in them. The use of abbreviations (where these are not standardised or agreed) and jargon should be avoided.

2.2 Passing information to partners, relatives or carers:

- When patients or clients are admitted to any Trust hospital/facility they must be asked for consent to pass on information about their condition and progress, including to partners, relatives or carers. If consent is refused this must be recorded in such a way as to ensure all staff answering enquiries are made aware of the patient’s or client’s wishes.

- Patients or clients attending outpatients or other clinics, whether health or social care related, must also be asked for consent before information about their condition/progress is passed to partners, relatives or carers.
• If a patient or client is unable to give consent (e.g. unconscious or otherwise unable to understand what is required), information about his/her condition must only be given to the person who is judged to be the next of kin. This would usually be the spouse or partner. In the case of a widow or widower or someone without a partner, the parent and any children of that patient/client have an equal right to information. If none of these relationships exist, a brother or sister would have a right to information. Outside of this, advice should be sought from the Data Guardian before passing on information to other relatives. Staff must be particularly sensitive when passing information about patients or clients with a learning disability. In limited circumstances it may be appropriate to share information or discuss a patient/client’s care with someone who has a formal caring role for that individual. This must only be done where it is clearly seen to be in the best interest of the patient/client. Information shared must be limited only to that which is required for the ongoing care of the patient/client.

• It is recommended good practice, in the case of patients or clients unable to give consent that a record is made of the information provided and to whom it has been provided. If the patient/client subsequently becomes fit to consent, he/she must be advised of the information that has been given and to whom it has been given, and must be asked for consent to continue to pass on information.

• Patients/clients over 16 are entitled to the same duty of confidence as adults and must be asked for consent to pass information to relatives, carers, etc. Patients under 16 who have the capacity and understanding to take decisions about their own treatment (‘Gillick competent’) are entitled also to decide whether personal information may be passed on and generally to have their confidence respected. In these circumstances professional staff will be consulted.

• Patient or client information, including condition reports and future appointment dates, should not be given out over the telephone unless permission has been given by the patient or client, or there is no doubt as to the caller’s entitlement to the information. As a general rule only basic information should be provided although it may be appropriate to provide more detailed information to immediate family members entitled to information who live a distance away. In all cases, staff must be satisfied that the person has a right to the information and that the patient or client has not objected.
• It is recognised that it may be necessary in A&E departments to give limited information without consent in order to identify an unaccompanied unconscious or critically ill patient.

• It should be noted that it is not appropriate to comply with requests from partners, relatives or carers to *withhold* information from patients or clients about the nature of their condition or the prognosis. Patients and clients have a right to this information and the Trust has no right to withhold it and must advise partners, relatives or carers accordingly. The need for great sensitivity in providing information to patients in situations where the prognosis is poor, cannot, of course, be over emphasised.

2.3 **Photographic, audio, and video recordings of patients/clients:**

• In all cases, of photographic, audio and video recordings, consent is required and refusal to participate must be respected. Consent can be given verbally and recorded and dated in the patient’s or client’s notes. The completion of a consent form is recommended where recordings or images are likely to be published. In both cases, the patient or client must be informed, in a way he/she can understand, why the recording/images are being taken and how they will be used. Otherwise consent will not be valid. The person responsible for seeking consent is the person requesting the image or recording.

• Images taken as part of care and treatment are confidential. A hard copy must be placed in the patient’s/client’s record and must be protected in the same way as any other confidential document within a health or social care record. Once the hard copy is made, the image must be deleted from the camera/PC.

• Staff from the Medical Illustration Department, the Communications team and other Trust staff with responsibility for taking photographs/videos or audio recordings of patients or clients, are prohibited from doing so without first having sight of a completed and signed consent form or a record of the consent in the patient’s/client’s notes. Agreement to take photographs and the use of the images should be explicitly discussed with patients / clients and consent should be recorded.

• If a staff member’s phone has a camera it should not be used in the workplace. For reasons of privacy and confidentiality, service users, relatives and other visitors should also be discouraged from using personal phones or cameras to take photographs on Trust premises.
2.4 Secondary Use of Personal Data and Research studies:

In accordance with the guidelines issued by the DHSSPS Executive in “The Code of Practice on Protecting the Confidentiality of Service User Information”, the Trust must ensure that when sharing service user identifiable data for non direct care (secondary purposes), assurances are provided by the requesting organisations that they comply with the Data Protection Act (1998) and that they have relevant DP Policies and Procedures in place which their staff are aware of. A Data Access Agreement must be completed by any organisation wishing to access Trust personal data for secondary purposes. It must be considered for approval and signed by the Trust’s Personal Data Guardian.

Personal Identifiable information should not be transferred to, stored or processed on any personal computer external to the HSC unless a Data Access Agreement is in place and the necessary ICT security measures have been agreed. Staff should refer to the “DHSSPS & HSC Protocol for Sharing Service User Information for Secondary Purposes (2011)”

Researchers undertaking studies and who require access to patient identifiable information and / or anonymous HSC data should follow the research protocol (Research Governance Framework for Health and Social Care in Northern Ireland).

See Appendix 6 for principles to be followed when considering use and disclosure of service user information.

2.5 Access to records: Patients and clients, or their representatives, have a right of access to see or obtain copies of their health and social care records under the Data Protection Act 1998. All such requests should be responded to positively and, if possible, patients or clients attending clinics or being seen by health or social care professionals should be allowed to see their records, without charge. Applications for access to the records of deceased patients or clients will be dealt with under the Access to Health Records (NI) Order 1993 (AHR). Further information and guidance is available on the Trust Intranet.

All requests for patient/client records (under DPA / AHR) will be dealt with centrally by the ‘Information Governance Office’ based in the Tyrone & Fermanagh Hospital, Omagh. These will be processed under the Trust’s ‘subject access’ procedures. When information has been approved for release, a copy of relevant notes / records only should be provided. Original records should not be released unless a Court Order is received requiring this.
Staff also have a right of access under the Data Protection Act to see and receive copies of their personal information held by the Trust. All such request must be responded to positively and within the time limits set out in The Act.

(see Appendix 3 for further information on ‘subject access’ and ‘redaction’)

2.6 **Use of computerised patient/client information systems:** All patient/client information system users must adhere to the attached protocol (Appendix 4).

2.7 **Confidential Information by fax or e-mail:**

Staff should refer to the Trust’s ‘Electronic Transmissions Protocol’ for direction and guidance on the use of fax machines or email for sending confidential information, including the electronic transfer of person-identifiable data and other confidential information.

**Use of Fax Machines:** Due to increased risks to the confidentiality and security of personal information, fax machines must not be used to transmit personal identifiable data or other confidential information unless in exceptional circumstances and approved by the Head of Department. Any circumstances where the use of fax for sending personal information is deemed acceptable should be outlined in departmental procedures. Fax machines must not be used for the routine transmission of sensitive personal identifiable data. Circumstances under which confidential information can be transmitted by fax are outlined in the Electronic Transmission Protocol. In circumstances where departmental procedures have deemed it acceptable to use fax as a method for sending personal / confidential information, ‘safe haven’ fax procedures should be followed. In all cases, only the minimum information must be sent by fax and great care must be taken to ensure the correct fax number is used and the intended recipient’s details are recorded on the fax cover sheet.

**Use of Email:** Personal-identifiable information sent by email within the Western Trust or to Trusts and other agencies within the HSC must be done within the requirements of the Data Protection Act and individual staff members are responsible for ensuring the confidentiality of information they send by email. Information can be transferred across the HSC email network in the knowledge that the system is secure and protected, however staff should still protect any file attachments that are sensitive or contain personal/patient level information. ‘Safe email transmission procedures’, as outlined in the Electronic Transmission Protocol, should be followed.
Personal-identifiable information must *not* be sent by email outside the HSC network unless proper security measures, approved by the Trust ICT department, are in place, including encryption and pass-word protection of data. (See 2.4 - Data Access Agreement).

In all cases, only the minimum information must be sent by email and great care must be taken to ensure the correct email address is used.

Personal information about service users or staff should not be emailed either to or from any staff member’s personal computer or personal email account.

**2.8 Use of portable PCs and devices:** No identifiable data may be stored on laptops or devices such as USB sticks, unless protected by encryption software recommended by the ICT Department. Portable PCs containing identifiable information must be locked away when not in use and staff using portable PCs with this type of information must take all reasonable steps to guard against theft or loss and against unauthorised use. Further information on portable PC management and security is available from the Head of ICT.

**2.9 Police enquiries:** The Police do not have an automatic right of access to patient or client identifiable information. There is an exemption in the Data Protection Act that allows you to give out personal information because it is needed to prevent or detect a crime, or catch and prosecute a suspect but there are limits on what you can release (Section 29 – Crime and Taxation). The police are most likely to ask the Trust to release personal information under this exemption; however requests may also be received from other organisations that can rely upon this exemption because they have a crime prevention or law enforcement function (e.g. benefit fraud).

Requests from the police or other organisations under section 29 of the DPA should be submitted in writing, for consideration by the Trust. It is preferable that the request is accompanied by the written consent from the data subject to release his/her information. Where it is not possible for this authority to be provided, full reasons for requesting the information should be provided in writing and clearly specify the relevant information required. For requests from the Police Service of Northern Ireland this will normally be on a PSNI ‘Form 81’ – Request for disclosure of personal data. When dealing with a request under section 29, Trust staff should consider what information can reasonably be released for the stated purpose. Any required redaction (see appendix 3) should be completed before information is released.

For further guidance on what you need to consider when you are asked to release personal information to the police or other organisations under section 29
of the DPA, see the Information Commissioner’s website (www.ico.org.uk) – “Releasing information to prevent or detect crime (section 29)”.

When information has been approved for release to the Police, a copy of relevant notes / records only should be provided. Original records should not be released unless a Court Order is received requiring this.

**2.10 Media enquiries**: Patient or client consent must be obtained before passing identifiable information, including condition reports, to the media. All media enquiries must be directed to the Head of Communications.

**2.11 Removal of patient/client records from Trust premises by staff**: The removal of patient/client records from Trust premises by staff, except in the following circumstances, is prohibited:

- When a patient/client is being transferred for care or treatment to another hospital/Trust.
- When a member of staff is making a domiciliary visit and must take a patient’s or client’s notes along.
- When notes are needed for evidence in a court case and the attending member of staff cannot collect them on the day of the hearing.
- When a consultant or other professional has a clinic outside Trust premises, or is attending another hospital, and needs to take notes home overnight.
- When other working practices require professional staff to take records home overnight (to be returned to Trust premises the next working day).

With regard to the above situations in which the removal of patient/client records from Trust premises is permitted, consultants or other staff involved are required to ensure the notes are either tracked, or their removal from the premises is otherwise recorded, and that everything possible is done to safeguard them from unauthorised access, loss, or damage and to return them to their place of origin as quickly as possible.

In the case of patient transfers to another hospital, the Trust Policy – “Inter Hospital Transfer of Patients And Their Files/Records (July 2008)” and CREST ‘Protocol for the inter-hospital transfer of patients and their records’ (August 2006) must be followed. Key principles are:

- Either the patient’s record or a written note of the patient’s condition, including all relevant factors, must accompany every patient being transferred to another hospital. If the patient’s record is being transferred, it must be tracked to the receiving hospital.
ii. The drug kardex, or a photocopy - not a transcription – must also go with the patient.

iii. Staff must, as a matter of routine, check, both by reading the patient’s armband and by asking the patient to confirm his/her identity (if possible), that they are sending the right notes with the right patient.

2.12 CCTV images: The use of CCTV cameras in certain areas of Trust premises to protect staff and prevent crime is permitted. Staff responsible for the management of CCTV equipment are required to comply with the requirements of the Information Commissioners code of practice on CCTV and data protection. This will include reviewing the need for cameras on a regular basis, the proper siting of cameras, and effective administration in respect of the storing, viewing, disclosing and retaining of images.

2.13 Retention and destruction of identifiable information: The DPA requires that patient and client information is kept for no longer than is necessary and is safely destroyed when the purpose for which it was first created is fulfilled.

Minimum retention periods: Staff should comply with the Trust’s Records Management Policy and DHSSPS document ‘Good Management Good Records’ (GMGR) (www.dhsspsni.gov.uk/) in relation to the retention and disposal of all Trust records. Before disposing of any Trust records staff should check the latest GMGR guidance for how long a record needs to be kept and also for the approved method of disposal (final action). e.g. destroy the record(s) or transfer to the Public Records Office of Northern Ireland (PRONI) if deemed of historical value / interest..

Confidential Waste: Staff should ensure that they follow the Trust’s Waste Manual for the disposal of any confidential papers relating to or identifying individuals (patients, clients or staff) and other confidential Trust business. Confidential paper for disposal should either be shredded (using a cross cut shredder) or where shredders are not available they should be in placed in a Confidential Waste Bag. Confidential waste bags must be stored in a designated secure area in the facility out of public view and accessibility until removed for appropriate disposal. Managers should ensure that procedures are in place within individual offices, departments or wards to ensure the Waste Manual is followed.

2.14 Reporting Missing Records: When patient/client records are reported as missing, all internal searches and checks should be carried out by the staff involved in accordance with departmental procedures. Searches may involve contacting other departments, wards, teams or facilities if appropriate to assist in
the searches. The Head of Department must be notified at the earliest opportunity and an incident report completed if the record cannot be located within a reasonable time. Tracking/Tracer systems must be updated to advise that the original record is missing and also if it is found.

2.15 **Social Media:** Trust staff should refer to the Trust’s ‘Social Media Policy’ for advice and guidance on the appropriate use of social networking sites. Staff should never share confidential information online, including identifiable personal information about patients, clients or other employees (including photographs), or confidential Trust business. Staff should never post inappropriate comments about employees, patient or clients on social networking sites.

2.16 **Transporting Confidential Information:** Staff should ensure that confidential information, especially identifiable information about patients/clients and staff, is always transferred by secure means, whether internally within the Trust or external to the Trust. If information is being transferred to other departments, including departments within the Trust that are in relatively close proximity, it must always be either hand-delivered directly to the intended recipient or securely packaged and clearly addressed, with senders details provided. This is the minimum requirement for posting sensitive patient/client/staff records however individual departments should consider other measures or procedures to ensure information is transferred safely and securely (e.g. order post-safe envelopes, reusable mailing pouches, etc. or develop internal department procedures for the regular transfer of records).

For further guidance staff should refer to the Trust “Records Management Good Practice Guidance - Transporting Records”; and to the General Code of Practice on confidentiality (appendix 5 of this policy)

2.17 **General code of practice on confidentiality:** The attached Trust code of practice (Appendix 5) is aimed at all staff working closely with patient and client records.

**SECTION 3: HOLDING AND PASSING ON PATIENT OR CLIENT INFORMATION**

The following principles, drawn from the Caldicott Report 2013, must be upheld in respect of the holding and passing on of patient or client information to organisations within and outside the HSC.

3.1 No identifiable information will be held or used without justification. (See paragraphs 3.4 below for justifiable purposes)
3.2 the minimum necessary identifiable information will be held, used, and passed on for justifiable purposes (see below).

3.3 Access to identifiable information must be on a strict need to know basis.

3.4 In order to secure the principles at paragraphs 3.1 – 3.3 (above), the following will apply within the Trust:

a. All identifiable information, including anonymised information, will only be passed on for a justifiable purpose. Justifiable purposes include:

1. delivering personal care and treatment;
2. assuring and improving the quality of care and treatment (e.g. through clinical audit);
3. training and educating staff and students including doctors, nurses, radiographers, social workers and others involved in health and care professional training;
4. monitoring and protecting public health;
5. co-ordinating HSC care with that of other agencies (e.g. voluntary and independent services)
6. effective health and social care administration, in particular:
   • managing and planning services
   • paying doctors, nurses, dentists and other staff
   • auditing HSC accounts and preparing performance and other statistical information, including fraud investigation/detection and the work of external auditors appointed by HSC Health Services Audit.
7. management of risk;
8. investigating complaints and notified, or potential, legal claims
9. meeting statutory requirements or a court order.

b. Information must always be provided in an anonymised form when it is sufficient for a particular purpose.

c. The appropriate Trust’s Personal Data Guardians will be responsible for approving any transfer of patient/client identifiable information within or outside the Trust, which does not fall under the justifiable purposes listed above. The Personal Data Guardians, or a delegated officer with sufficient knowledge and seniority, will scrutinise the information request in accordance with Caldicott recommendations and the Information Commissioner’s ‘Framework code of practice for sharing personal information’ to ascertain the necessity for patient/client identifiable information to be used. If the Personal Data Guardian is not satisfied that patient identifiable information is
necessary, approval for use will be withheld. A data access agreement form must be completed and approved as part of this process (available on the Trust intranet site)
d. The Trust strictly prohibits the passing on or selling for fundraising or commercial marketing purposes any personal details of patients or clients, including names and addresses.

4. FURTHER HELP AND GUIDANCE: Staff should also refer to the DHSSPS “Code of Practice on Protecting the Confidentiality of Service User information” which is aimed at supporting staff in making good decisions about the protection, use and disclosure of service user information. See also the information leaflet “confidentiality of service user information - guidance for all staff working in health and social care in Northern Ireland”

Additional help and guidance on any aspect of this policy is available from the Trust’s Personal Data Guardians, the Assistant Director of Performance and Service Improvement and Trust Information Governance staff.

References:
- The Data Protection Act 1998
- The Code of Practice on Protecting the Confidentiality of Service User information (revised version: January 2012)
- The Access to Health Records (NI) Order 1993
- The Caldicott Report 2013
- DHSSPS Good Management, Good Records guidelines
- WHSCT Social Media Policy – April 2013
- WHSCT ICT Security Policies
- Good Practice Guidance from Information Commissioner’s office
  www.ico.org.uk
Relevant Legislation and Guidance

The Trust complies with the following legislation and guidance:

- the Data Protection Act (DPA) 1998;
- the Access to Health Records (NI) Order 1993;
- Code of Practice on protecting the confidentiality of service user information (revised version January 2012);
- the recommendations and principles contained within the Caldicott Report (2013);
- the Human Rights Act (HRA) 1998 (Article 8);
- common law related to the duty of confidentiality;
- the codes and standards on confidentiality laid down by professional bodies such as the BMA; NMC; RCPCH; GMC; HPC; and GSCC.
- DHSSPS guidelines: ‘Good Management Good Records’
- National Archives “Redaction toolkit (Editing exempt information from paper and electronic documents prior to release)

The Freedom of Information (FOI) Act 2000 contains an exemption to the release of personal information (Section 40). However, requests made under the FOI Act for access to personal information, especially requests for access to the applicant’s own information, should be dealt with under the DPA 1998. Requests for access to third party information are likely to be dealt with under the FOI Act. Further information on the FOI Act is available from the office of the Assistant Director, Performance and Service Improvement.
Guidance Notes:

i) The term ‘processing’ is defined in the Data Protection Act 1998 (DPA) as:

“Obtaining, recording or holding information or data … or carrying out any operation or set of operations including:

- Organisation, adaptation or alteration of the information;
- Retrieval, consultation or use of the information or data;
- Disclosure of the information or data by transmission, dissemination or otherwise making available; or
- Alignment, combination, blocking, erasure or destruction of the information or data.”

ii) The rights of individuals under the Data Protection Act 1998 (DPA) are:

1. Right of subject access (see below);
2. Right to prevent processing likely to cause damage or distress;
3. Right to prevent processing for the purposes of direct marketing;
4. Rights in relation to automated decision-taking;
5. Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller;
6. Right to take action to rectify, block, erase or destroy inaccurate data; and
7. Right to make a request to the Information Commissioner for Data Protection for an assessment to be made as to whether any provision of the Act has been contravened.

iii) Right of ‘subject access’

Under DPA, patients, clients and staff (or their representatives) have the right to see and have copies of information held about them.

With regard to deceased persons, the governing legislation is the Access to Health Records (NI) Order 1993.

Trust ‘subject access’ procedures will be available on the Trust Intranet site.
iv) **Redaction:** Redaction is the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. It can be used when one or two individual words, a sentence or paragraph, a name, address or signature needs to be removed before a document is released. Further guidance on how to redact a document is available from the National Archives “Redaction toolkit (Editing exempt information from paper and electronic documents prior to release). [http://www.nationalarchives.gov.uk/documents/redaction-toolkit.pdf](http://www.nationalarchives.gov.uk/documents/redaction-toolkit.pdf).

v) **Senior Information Risk Owner (SIRO); Information Asset Owner (IAO); and Personal Data Guardian (PDG)**

The SIRO and the PDG roles are distinct and separate within the Trust, however the SIRO and IAOs will work closely with the PDGs and consult him/her where appropriate when conducting information risk reviews for assets which comprise or contain patient/client information.

The SIRO is a member of the Trust Board who is responsible to ensure organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist. The SIRO will provide advice to the Accounting Officer (Chief Executive) on the information risk aspects of the Statement of Internal Control.

**The SIRO:**
- Is accountable
- Fosters a culture for protecting and using data
- Provides a focal point for managing information risks and incidents
- Is concerned with the management of all information assets

**The PDG:**
- Is advisory
- Considers the principles and ethics around the use of data
- Provides a focal point for patient/client confidentiality & information sharing issues
- Is concerned with the management of patient/client information

**IAO:**

The IAO role will lead and foster a culture that values, protects and uses information for the public good. They will support the SIRO function by understanding what personal information is held in all systems across the Trust (manual and electronic). They will be directly accountable to the SIRO and will provide assurance that information risk is managed effectively for the information assets that they own.
Appendix 4

TRUST PATIENT AND CLIENT INFORMATION SYSTEMS DATA PROTECTION PROTOCOL

The following applies to all users of Trust computerised patient and client information systems:

1. Staff with access to Trust patient/client information systems are required to maintain the highest level of confidentiality and to guard against unauthorised access. They must only use the system for the purpose(s) for which it is intended to be used and on no account should they access patient or client information for personal or any other unauthorised reason. Staff must not share their system password with others and if they believe that someone else knows or may know their password, they must change it immediately and inform the IT System Support Manager. Staff who fail to follow the requirements of this protocol and of the Trust's data protection and confidentiality policy face disciplinary action, including termination of employment, and may also face individual prosecution under the Data Protection Act 1998.

2. Any system output (printouts, letters, etc.) containing identifiable information must be handled extremely carefully to protect patient/client confidentiality and must be destroyed after use (see paragraph 3) or, if necessary, filed carefully away in accordance with agreed retention period.

3. All forms of identifiable output from patient/client information systems must be either shredded, using cross-shredders only, or incinerated, or in the case of discs, tapes, etc. must be wiped clean or shredded on the advice of the IT Security Manager. In no circumstances must sensitive waste of this nature be placed in the normal rubbish collection or re-used without obliterating identifiable information.

4. If identifiable hard copy information is being transferred to other departments, including departments within the Trust that are in relatively close proximity, it must always be either hand-delivered directly to the person who is to receive it, or sent in a sealed envelope, carefully addressed and marked 'confidential' and 'internal mail'.

5. Staff must refer to the Trust policy ‘Data Protection and Confidentiality’ policy, Email Policy and to the Trust protocol governing electronic data transfers and must seek advice before transferring any identifiable information externally, whether within or outside the HSC.
6. Office/ward/department managers and supervisors should ensure that photocopiers, printers and VDU screens are not visible to unauthorised personnel. It is particularly important that patients/clients or visitors to Trust facilities cannot view screens.

7. Identifiable information must be locked away when not in use and destroyed as outlined in paragraph 3 above when its purpose is fulfilled. No identifiable material should be left out overnight or at times when the area is unmanned. The last person to leave a work area at any time should quickly check that all material of a sensitive nature has been locked away.

8. It is recommended that paper documents from which personal/clinical data is being inputted are marked (e.g. by initialling) to denote that the data has already been inputted and to avoid duplication.

9. It is important that every opportunity is taken, including checking with patients and clients directly when they attend Trust premises, to ensure that information held is up-to-date and accurate.
CONFIDENTIALITY – TRUST GENERAL CODE OF PRACTICE

1. Background

Many staff working in Health and Social Care have access to personal information relating to patients, clients or staff. All of this information is strictly confidential. Information about patients and clients is particularly sensitive and carries an enhanced duty of confidentiality. Staff who breach confidentiality face disciplinary action, including termination of employment, and may also face individual prosecution under the Data Protection Act 1998. Staff are required to familiarise themselves with the requirements of the Trust policy – ‘Data Protection and Confidentiality’

2. General rules

a) When working with personal confidential information whether on paper or computer, refer only to those sections to which you need to refer in order to do your job. Personal information about patients, clients or staff should only be used for the purpose for which it was collected, unless otherwise approved.

b) Ensure that all information that can identify an individual or individuals (lists, labels, forms, etc.) is properly secured away from anyone who is not entitled to access it and is safely destroyed after use.

c) All personal information should be filed securely and accurately, particularly within patient/client files and care should be taken to ensure information is not misfiled in another person’s chart.

d) All documentation holding identifiable patient/client information, including for example diaries, message books, notebooks, appointment books, registers etc should be kept confidential, stored securely and retained for the appropriate length of time, in line with the Trust disposal schedule.

e) Confidential information, including identifiable information about service users and staff, should always be transferred by secure means, whether internally within the Trust or external to the Trust. If identifiable hardcopy information is being transferred to other departments including departments within the Trust that are in relatively close proximity, it must always be either hand-delivered directly to the person who is to receive it or sent in confidential mail bags or in a sealed envelope. All packages containing personal
information should be carefully addressed and marked “Confidential” (and where relevant “Internal Mail”). The name of the addressee and the full postal address should be confirmed and clearly written on the front of all envelopes/packages containing personal information. A ‘return to sender’ address (if undelivered) should be clearly marked on the reverse of the envelope/package. Further guidance can be found in the Trust “Records Management Good Practice Guidance - Transporting Records”.

f) Keep computer screens showing personal information turned away from general view. Always log off when leaving the computer. Do not give anyone else your computer password.

g) Do not allow anyone access to personal confidential information unless you are sure of their right to have access. Never assume because a person looking for access is a doctor or a nurse, or a senior manager, etc. they have a right of access. If in doubt, check with your line manager.

h) Do not divulge information about anyone – patient, client or staff member - over the telephone, even if it is only an address or a date of birth, without assuring yourself of the caller's right to that information.

i) If you have to ring a patient or client at home, be very discreet. Ensure you are talking to the patient or client. If he/she is not available, call back rather than leave a message.

j) Always use the ‘mute’ or ‘secrecy’ button on the telephone when putting a caller on hold so that business conversations in the office/ward/department that might be about patients, clients or staff are not overheard.

k) Do not talk about patients, clients, or staff other than to provide necessary information. Remember in the case of patients and clients, even mentioning the fact that a person is attending the hospital or another Trust facility may constitute a breach of confidentiality.

l) When talking directly to patients or clients to check personal details, be discreet. If you can be overheard, keep your voice as low as possible when asking questions. People who are hard of hearing may need to be taken to one side in order to get the necessary details. Whenever possible, hand the person his/her written details and ask him/her to check the accuracy. But some people may not read very well and computer print is sometimes less than clear so be prepared to help, discreetly and sensitively.
m) Records containing sensitive personal information about patients, clients or staff should be stored securely and out of public view and only accessible to appropriate Trust staff.

n) Confidential waste should be disposed of securely and in line with the Trust’s Waste Manual and office procedures (i.e. either shredded or where shredders are not available they should be in placed in Confidential Waste Bag provided). Confidential waste bags must be stored in a designated secure area until removed for appropriate disposal.

o) Staff should follow the Trust’s ‘Electronic Transmissions Protocol’ when sending confidential information by fax or email.

p) Confidential / personal identifiable information should not be emailed to or from any staff member’s personal email account; and should not be stored or processed on any staff member’s personal computer.

q) The removal of patient/client records from Trust premises by staff is prohibited, except in the circumstances outlined in the Data Protection & Confidentiality Policy relating to patient/client care (section 2.11). Information sheets such as ‘handover notes’ used staff working with inpatients should not be taken home and should be confidentially destroyed when no longer needed.

r) At every opportunity staff should check with patients and clients directly to ensure that information held is up-to-date and accurate. Systems and records should be updated accordingly.

s) Staff should never post confidential information or any inappropriate comments about patient, clients or other employees on social networking sites.

**REMEMBER:** Patients, clients and staff have a right to have their information held in confidence. Patients and clients have an enhanced right because of the sensitivity of the information we hold about them. All staff have a legal duty to protect that confidentiality. Regardless of seniority, job title or profession, no one has an automatic right to access confidential information, especially information about patients or clients. If in doubt, do not give out information but seek your supervisor’s/line manager’s advice.
### Principles Governing Information Sharing

<table>
<thead>
<tr>
<th>Code of Practice 8 Good Practice Principles&lt;sup&gt;2&lt;/sup&gt;</th>
<th>DPA Principles</th>
<th>Caldicott Principles&lt;sup&gt;3&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. All organisations seeking to use confidential service user information should provide information to service users describing the information they want to use, why they need it and the choices the users may have.</td>
<td>1. Data should be processed fairly and lawfully.</td>
<td>1. Justify the purpose(s) for using confidential information.</td>
</tr>
<tr>
<td>2. Where an organisation has a direct relationship with a service user then it should be aiming to implement procedures for obtaining the express consent of the service user.</td>
<td>2. Data should be processed for limited, specified and lawful purposes and not further processed in any manner incompatible with those purposes.</td>
<td>2. Only use it when absolutely necessary.</td>
</tr>
<tr>
<td>3. Where consent is being sought this should be by health and social care staff who have a direct relationship with the individual service user.</td>
<td>3. Processing should be adequate, relevant and not excessive.</td>
<td>3. Use the minimum that is required.</td>
</tr>
<tr>
<td>4. ‘Third Party’ organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data.</td>
<td>4. Data must be accurate and kept up to date.</td>
<td>4. Access should be on a strict need-to-know basis.</td>
</tr>
<tr>
<td>5. Any proposed use must be of clear general good or of benefit to service users.</td>
<td>5. Data must not be kept longer than necessary.</td>
<td>5. Everyone must understand his or her responsibilities.</td>
</tr>
<tr>
<td>6. Organisations should not collect secondary data on service users who opt out by specifically refusing consent.</td>
<td>6. Data must be processed in line with the subject’s rights (including confidentiality rights and rights under art. 8 of Human Rights Act).</td>
<td>6. Understand and comply with the law.</td>
</tr>
<tr>
<td>7. Service users and/or service user organisations should be involved in the development of any project involving the use of confidential information and the associated policies.</td>
<td>7. Data must be kept secure and protected against unauthorised access.</td>
<td></td>
</tr>
<tr>
<td>8. To assist the process of pseudonymisation, the Health and Care Number should be used wherever possible.</td>
<td>8. Data should not be transferred to other countries without adequate protection.</td>
<td></td>
</tr>
</tbody>
</table>

---

<sup>1</sup> These principles must be followed by health and social care organisations when considering use and disclosure of service user information.

<sup>2</sup> Code of Practice, paragraph 3.17.

<sup>3</sup> PDG Principles are adopted from the Caldicott Principles established in England and Wales.