Western Health and Social Care Trust

Data Protection and Confidentiality Policy

November 2018

Western Health and Social Care Trust

Policy Title:	Data Protection & Confidentiality Policy
Policy Reference No:	Corp11/003
Original Implementation date:	March 2008
Revised:	March 2011
	November 2013
	November 2015
	November 2018 (deferred from Nov 2017 due to impending new legislation)
Next review date:	August 2020
Responsible Officer:	Assistant Director of Performance & Service Improvement

Western Health and Social Care Trust

Table of Contents

1. Introduction

The Western Health and Social Care Trust is fully committed to complying with the Data Protection Act 2018 (DPA) and the EU General Data protection Regulation (GDPR) which came into force on 25 May 2018. This policy sets out responsibilities and provides a set of principles covering all aspects of processing personal data or personal information. (see Appendix 3 for definition of 'processing').

Health and social care information is defined by data protection legislation as "special category data" which is considered to be more sensitive and as such requires 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/GDPR. This legislation 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 data protection legislation, 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 and volunteers working in, or for, the Trust are subject to the same duties of confidence. Clinical, social care, professional 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 (permanent, bank and temporary), volunteers, 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 data protection legislation.

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 the DPA / GDPR 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 principles of the GDPR. In summary, this means personal information must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject - (Lawfulness, Fairness and transparency). There must be valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data and you must not do anything with the data in breach of any other laws. Personal data must be processed in a way that is fair and not unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes – (Purpose limitation)

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed - (data minimisation)

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are

processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject – (Storage Limitation)

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

In accordance with Article 5(2) of the GDPR the Trust shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above (Accountability).

Our purpose for holding personal information, along with a description of the categories of people and organisations to which we may disclose it, are included in our Privacy Notice. This is available electronically on the Trust website, in printed format in Trust facilities or by asking a member of staff.

The Trust is registered as a Data Controller with the Information Commissioners Office (ICO)**. ICO Registration Number – Z9827264**

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 and the necessary safeguards or contractual arrangements are in place. Respect to confidentiality will be given where appropriate.

Special Category personal data will only be disclosed or collected where a lawful basis specific to Special Category data, as defined by Data Protection Legislation, is met.

Personal data will only be disclosed outside of the EEA where additional conditions as defined by Data Protection Legislation are met.

The Trust will always endeavor to ensure there is a lawful basis, as set out in Articles 6 and 9 of GDPR, for processing personal information. It 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).

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 and as outlined in the staff privacy notice. 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;
- the information is clearly not intrusive in nature;
- the member of staff has consented to the disclosure;
- 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 data protection 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 accuracy and quality of personal information used;
- where possible pseudonymise or anonymise personal identifiers within information held
- 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 (see Appendix 3);
- take appropriate technical and organisational security measures to safeguard personal information against any unlawful, unauthorised or accidental loss, damage, disclosure or destruction;
- ensure that personal information is not transferred abroad without adequate safeguards.
- be responsible and able to demonstrate compliance with all of the above

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 data protection legislation.

6. Compliance

The Trust will ensure that:

- appoint a Data Protection Officer (DPO) who will have specific responsibilities for Data Protection
- our purposes for processing personal data are clearly set out in Trust Privacy Notices so that patients, clients and staff are pro-actively informed of the uses to which their information is put.
- consent is sought before passing personal identifiable information on for any reason other than to fulfil justifiable and lawful purposes;
- all Subject Access Requests (SARs) will be dealt with in accordance with Data Protection legislation and within the legal timeframe of 1 month. ;
- new staff receive training in data protection as part of their induction and existing staff are reminded of their data protection obligations and provided with awareness training at least every 3 years.
- 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 personal data breach of and a breach of 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 Personal Data Guardian.
- Personal recording equipment, e.g. employees' own cameras or smartphones, are not permitted to be used for the recording of patient images or data
- CCTV systems are used and managed in accordance with the Trust's CCTV Policy and the Information Commissioners 'CCTV data protection code of practice' (see Appendix 1 - section 2.13)
- 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;
- a Trust Information Asset Register (IAR) is in place to record what personal information assets are held, how they are processed, maintained and managed
- a DPIA is completed as part of the 'data protection by default and by design' approach to new systems or processes where there is likely to be a high risk to the privacy of the individuals involved. (see guidance notes at Appendix 3)

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 (DPO) responsible for monitoring compliance; providing advice and guidance; dealing with escalated complaints from data subjects; liaising with the ICO and Trust Solicitors on data protection issues
- created a Data Protection Policy and associated procedures and protocols providing detailed guidance on data protection issues; and
- a mandatory awareness and training programme in place, to include induction training and regular refresher training (including eLearning), 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.
- arrangements in place for reporting and investigating any personal data breaches (see App 1: section 2.17)
- continued to work collaboratively with the DoH and other HSC organisations to agree and develop regional approaches to data protection requirements.

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 Data Protection Act / GDPR. There will be an expectation that these parties will audit their compliance with data protection legislation and will provide assurances to the Trust in this respect.

Responsibilities regarding DPA compliance must be covered off as part of any contracts, Service Level Agreements (SLAs), Data Sharing/Access Agreements (DSAs / DAAs) and MOUs with third parties.

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 Trust computers, mobile devices and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically. Access controls should also be placed on electronic records containing personal and sensitive information.
- No personal data about Trust patients, clients or staff is transferred to or held on personal computers of staff members.
- 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 Guardian** (PDG) role is advisory and will consider the principles and ethics around the use of personal data. The PDG will provide a focal point for patient/client confidentiality and information sharing issues. The Trust PDGs 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 2018, GDPR 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 2018, GDPR and associated legislation. Directors are also responsible for ensuring that breaches of the DPA/GDPR 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 fulfil the role of Senior Information Risk Owner (SIRO) and will also have a particular interest in respect of ICT security policies to ensure the proper protection of personal information held electronically.

Senior Information Risk Owner (SIRO) and Information Asset Owners

The SIRO is accountable for information risk management and will foster a culture for protecting and using data. The SIRO provides a focal point for managing information risks and incidents and is concerned with the management of all information assets.

The SIRO and 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 Assistant Directors (all directorates) as Information Asset Owners (IAO) will lead and foster a culture that values, protects and uses information for the public good. IAOs will support the SIRO function by understanding what personal information is held in all systems across the Trust (manual and electronic), the purpose of information assets within their area of responsibility and ensure the Trust's Information Asset Register is accurate and up to date. They will assess the risks for the information assets that they own and provide an annual assurance to the SIRO that the information risk is managed effectively.

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/GDPR and the routine monitoring of DPA/GDPR 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 and will deputise for the SIRO in her absence.

The Data Protection Officer (DPO) will assist the Trust to monitor internal compliance, inform and advise on data protection obligations, provide advice to staff and service areas on Data Protection issues including Data Protection Impact Assessments (see guidance notes at Appendix 3) and act as a contact point for data subjects and the supervisory authority (ICO).

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 2018 / GDPR to manual as well as computer held records, and the resulting implications. *All* directors, assistant directors, Information Asset Owners and other 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 (when appropriate to do so), 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 and associated protocols / procedures 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 Privacy Notice is freely available in all patient and client waiting areas and other suitable areas within the Trust. Every opportunity should be taken to provide privacy information to patients and clients, such as including it in relevant publications and correspondence, issuing with appointment and admission letters and making 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. Managers must also ensure that staff complete refresher training on data protection at least every three years.

A copy of this policy and associated policies and procedures 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 2018 and the GDPR and associated legislation and guidance. Staff should take all necessary steps to ensure that personal information held in all formats (paper and electronic) is kept safe and secure at all times and protected against loss, damage or inappropriate disclosure.

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 data protection legislation, 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.
- Records containing personal information should be kept secure at all times and locked away when not in use.
- Care should be taken to avoid misfiling and use proper checks to ensure that information is filed in the correct persons chart.
- Appropriate action must be taken when misfiling has been identified.
- It is the responsibility of every individual who has access to patients' notes to ensure that all information contained within the notes is pertinent to that individual patient.

- Personal information should not be retained for longer than is necessary. All records should be disposed of in accordance with DHSSPS guidelines.
- A record made in any format (e.g. written, audio or visual) of meetings with patients, clients or staff must be treated as confidential and processed in accordance with Data Protection legislation and other relevant policies / guidelines
- Staff should follow best practice as outlined in the Trust's Records Management Policy and professional guidelines on record keeping.

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.

- Children need particular protection when collecting and processing their personal data. The concept of competence (the child's capacity to understand the implications of their decisions) is valid under the DPA / GDPR legislation. If a child is not competent to exercise their own data protection rights or consent to processing themselves then it will usually be in their best interests to allow an individual with parental responsibility to act on their behalf. If a child is competent then your overriding consideration should still be what is in their best interests however, in most cases it should be appropriate to let the child act for themselves.

  Children are entitled to the same duty of confidence as adults and when appropriate should be asked for consent to pass information to relatives, carers, etc. Children 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.

- Personal recording equipment, e.g. camera or smartphone, are not permitted to be used for the recording of patient images or data

- Service users, relatives and other visitors are not permitted to photograph or video staff members without their consent.

- Staff should also follow ethical guidance provided by professional bodies on visual and audio recordings of patients made and used in a professional capacity.

  - as part of a patient's care
  - for teaching, training, or assessment of health professionals and students

- for research and development
- for use in widely accessible public media, such as on the internet or broadcast on radio or television.

For example - reference:

- www.gmc-uk.org/guidance/ethical_guidance/making_audiovisual.asp
- www.nmc-uk.org - guidance on using social media responsibly.
- https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-governance-and-technology-resources The Use of Mobile Devices in Hospitals (e.g. Phones, Tablets and Cameras)

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 Data Protection legislation 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).

Where appropriate, applicants should be referred to the Honest Broker Service (HBS) which enables the provision of anonymised, aggregated and in some cases pseudonymised health and social care data to the DHSSPS, HSC organisations and in the case of anonymised data for ethically approved Health and Social care related research.

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

2.5 Access to records: Under data protection legislation, patients, clients or their representatives, have a right of access to their personal information, including a right to receive a copy of their own health and social care records. This is called a 'subject access request' (SAR). The Trust has procedures in place for dealing with all such requests, which should be responded to positively.

If possible, patients or clients attending clinics or being seen by health or social care professionals should be allowed to see their records.

Applications for access to the records of deceased patients or clients will be dealt with under the Access to Health Records (NI) Order 1993.

All requests under the above legislation for copies of patient/client records will be coordinated centrally by the Trust's '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 Data Protection legislation to see and receive copies of their personal information held by the Trust, either by the Human Resources department or by individual managers. All such requests must be responded to positively and within the time limits set out in GDPR.

In most cases, professional staff / managers will be required to review and authorise release the release of records. Staff that had previous involvement in the case may be consulted for their views on release. Where a staff member has left the Trust it is the responsibility of those with current responsibility of that service area to approve release of the notes and records. The removal / redaction of any information or details prior to release, should be performed or overseen by staff that are knowledgeable about the records or nature of the information / records and can determine what material is exempt.

(see 'Redaction Guidance' available on the 'Staff West' site)

2.6 Responding to Court Orders: Staff should refer to the Trust's Guidance on dealing with Court Orders (3rd party disclosure) when they receive correspondence from a solicitor or direction from a Judge to disclose a patient's or client's health and social care records in connection with an ongoing court case.

2.7 Police enquiries: The Police do not have an automatic right of access to patient or client identifiable information; however the Data Protection Act 2018 allows the disclosure of personal data to Police when the purpose is to prevent or detect crime or to safeguard the public.

The condition for the release of personal information is met if the processing –

(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and
(c) is necessary for reasons of substantial public interest.

Disclosure to Police is also permitted where the processing is necessary for compliance with the PSNI's legal obligation to safeguard the public (General Data Protection Regulations 2018 Article 6(1)(c)). This includes both statutory and common law obligations including Health and Safety. It is also permitted to disclose personal data where a risk to life exists, (Article 6(1)(d)).

The police are most likely to ask the Trust to release personal information for the above purposes; 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). Part 3 of the Data Protection Act 2018 allows for the processing of data by a competent authority for law enforcement purposes being *"the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".*

Requests from the police or other organisations for these purposes 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.

Requests from the Police Service of Northern Ireland will normally be submitted on a PSNI 'Form 81' – Personal Data Request Form.

When dealing with a request from the police, Trust staff should consider what information is proportionate and relevant to the issue being investigated; and what can reasonably be released for the stated purpose. Any required redaction (see appendix 3) should be completed before information is released.

When information has been approved for release to the Police, a copy of relevant notes / records only should be provided. Original records should only be released when a Court Order is received directing this.

2.8 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.

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

2.10 Confidential Information by fax or e-mail:

Staff should refer to the Trust's 'Protocol on Electronic Transmission of Confidential Information' 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 data protection requirements 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 Trust's Email Policy / 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. Always check email addresses before sending.

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.

2.11 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 and other hand-held devices (e.g. tablet computers) 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 / device management and security is available from the Head of ICT.

2.12 Removal of patient/client information 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.

Staff must ensure that work diaries, portable electronic devices and other mediums that contain personal information are kept secure at all times and protected against loss or unauthorised access.

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

i. 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.

In accordance with the Maternity Strategy 2012-2018 that all pregnant women in Northern Ireland will carry their own notes for the duration of their pregnancy, it is Western Trust policy that women will carry their own notes from the Antenatal booking until the postnatal period when the record is returned to the Hospital of origin. Records will then be retained by the Trust in line with DHSSPS retention and disposal guidelines (Good Management Good Records).

2.13 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. For further information see 'CCTV Policy'.

2.14 Retention and destruction of identifiable information: Data Protection legislation requires that personal data and information is not kept for longer than necessary (storage limitation principle) and that it is safely and securely destroyed when it is no longer needed.

Minimum retention periods: Staff should refer to and comply with the Trust's Records Management Policy and DHSSPS document 'Good Management Good Records' (GMGR) (https://www.health-ni.gov.uk/topics/good-management-good-records) 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.

2.15 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, including text messaging services / apps. 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 (internal or external to the Trust) however individual departments should consider other measures or procedures to ensure information is transferred safely and securely (e.g. order post-safe envelops, reusable mailing pouches, etc. or develop internal department procedures for the regular transfer of records).

2.17 **Reporting Personal Data Breaches:**

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Personal data breaches can be the result of both accidental and deliberate causes and is more than just about losing personal data.

Internal Reporting

In accordance with the Trust's "Incident Reporting Policy and Procedures", an incident report form should be submitted for all data breaches. It is the responsibility of the manager of the area where the data breach occurred, or those with responsibility for the information / records involved, to investigate the incident and up-date the Trust's incident reporting system (Datix).

Managers with corporate responsibility for particular areas should be informed of and/or involved in the investigation to ensure that appropriate action is being taken to resolve the issue and that learning is appropriately disseminated.

Further Reporting to the ICO

GDPR introduces a duty to report certain types of personal data breach to the Information Commissioner's Office (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible.

The Senior Information Risk Owner (SIRO) and the Head of Records and Information Governance and/or the Data Protection Officer will determine, whether the personal data breach should be reported further to the ICO after considering all relevant factors and the likelihood and severity of any risk to people's rights and freedoms, following the breach. Following assessment, if it is likely there will be a risk to rights and freedoms then the ICO will be notified within 72 hours. The decision on whether or not to report a breach to the ICO will be documented so that the Trust is able to justify the decision.

If a breach is likely to result in a 'high risk' to the rights and freedoms of individuals, those affected must also be informed directly and without undue delay so as to mitigate any immediate risk of damage to them and to help them take steps to protect themselves from the effects of a breach. The threshold for informing individuals is higher than for notifying the ICO and will be based on an assessment of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

In assessing risk to rights and freedoms, the Trust will focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Personal data breaches will be assessed on a case by case basis, looking at all relevant factors, including.

- Potential detriment to individuals (risk to rights and freedoms)
- Severity of the risk
- Volume of data affected
- Sensitivity of data
- Damage to reputation

Learning from all personal data breach incidents should be shared without breach of patient or staff confidentiality to minimise risk of a re-occurrence.

2.18 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.

2.19 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. coordinating 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 <u>always</u> 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 (DAA) 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" (January 2012) 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.

Appendix 2

Relevant Legislation

The Trust complies with the following legislation and guidance:

- the Data Protection Act (DPA)2018;
- the EU General Data Protection Regulation (GDPR)
- the Access to Health Records (NI) Order 1993;
- Code of Practice on protecting the confidentiality of service user information (January 2012)
- DHSSPS & HSC Protocol for Sharing Service User Information for Secondary Purposes (2011)
- 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'
- The Freedom of Information (FOI) Act 2000 *
- National Archives "Redaction toolkit (Editing exempt information from paper and electronic documents prior to release)
- Codes of Practice and Good Practice guidance from Information Commissioner's office www.ico.org.uk, including:
- ICO 'Data Sharing Code of Practice' (May 2011)
- "Good Administration and Good Records Management" guidance by The Northern Ireland Ombudsman and The Information Commissioner's Office (2014)

* 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 data protection legislation. 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.

Appendix 3

Definitions / Guidance Notes:

Personal data
The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data
The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). Special category data is personal data which is more sensitive, so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see GDPR Article 10).

Consent
'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Processing
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Pseudonymisation
'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Data Controller
'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Data Processor
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Third party
'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Data Protection Impact Assessment (DPIA)
DPIAs are a tool to help identify and minimise the data protection risks of new projects. They are part of the accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach. An effective DPIA helps to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur. A DPIA is mandatory when introducing a new system or process is likely to include a high risk to the privacy of the individuals involved.

Further guidance can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Individuals Rights

1) **The right to be informed** about the collection and use of personal data. This will be done through the provision of privacy information.
2) An individual's **right of access** to their personal data (subject access) within required timeframe as set out in legislation
3) An individual's **right to rectification** - to have inaccurate personal data rectified, or completed if it is incomplete
4) An individual's **right** to be forgotten' – the right to have personal data erased if it is no longer needed for the purpose for which it was originally collected (does not apply to if the processing is necessary for public health purposes in the public interest; or if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services).
5) **The right to restrict processing** in certain specific circumstances
6) **The right to data portability** in certain specific circumstances
7) **The right to object** in certain specific circumstances
8) **Rights in relation to automated decision making** (making a decision solely by automated means without any human involvement); **and profiling** (automated processing of personal data to evaluate certain things about an individual)

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. Redaction should be performed or overseen by staff that are knowledgeable about the records or nature of the records and can determine what material is exempt.

Further guidance on how to redact a document is available on the Trust StaffWest site (Redaction Guidance) and the National Archives "Redaction toolkit". http://www.nationalarchives.gov.uk/documents/redaction-toolkit.pdf.

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 appropriate ICT System 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 Data Protection legislation.
2. Any system output (printouts, letters, electronic downloads, 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, removable media (including Safe-Sticks) etc. must be wiped clean or shredded on the advice of the ICT 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. Care should be taken not to mix up information sent separately to shared printers. Where available, personal identifiable information (letters, reports, etc.) sent to a shared printer should be printed using the pin & print function. Information should always be checked to ensure it is not mixed up with information printed separately or by other staff. This is particularly important to avoid identifiable information being attached and inappropriately sent to the wrong person.

   Please refer to the guidelines available on the Staff West site for use of pin & print capabilities when sharing Multi-Function Printers (MFP's).

5. 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'.

6. Staff must refer to the Trust '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.

7. 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.

8. 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.

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

10. 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.

11. In order to keep personal information secure and protected against unauthorized access, staff should refer to the Trust's "Management of User Accounts and Password Policy" for guidance on the management and use of passwords on all Trust systems.

12. Staff should refer to the Trust's 'Protocol on Electronic Transmission of Confidential Information' for direction and guidance on sending confidential information by fax machines or email, including the electronic transfer of person-identifiable data printed or downloaded from Trust systems. (see also Appendix 1 point 2.10 of this policy)

13. The WHSCT - ICT INVESTIGATION REQUEST Form is to be used for ALL requests for information from ICT systems where inappropriate use is suspected and/or being investigated. All requests must be signed off by an Assistant Director / Information Asset Owner in the relevant directorate. The request will be approved by the Assistant Director of ICT & Telecommunications before an investigation is carried out on Trust systems and any information is provided by ICT

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 Data Protection legislation. Staff are required to familiarise themselves with the requirements of the Trust policies and protocols, including the 'Data Protection and Confidentiality Policy'; 'Records Management Policy'; and ICT security Policies;

2. General rules

a) Personal information should be accessed only on a 'need-to-know basis'. Staff must have a valid professional reason for accessing an individual's paper records or records held on computer, including patient based administration systems. Staff should not access their own records or results or those of a family member or friend, even if they ask you to.

b) 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.

c) 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.

d) All personal information should be filed securely and accurately, particularly within patient/client files. Files must be maintained in a neat and tidy, proper chronological order so information is easily found. There should be no loose papers in patient/client files.

e) Care should be taken to ensure personal information is not misfiled in another person's chart as this could lead to a clinical incident or data breach. Be extra careful when filing information for patients with the same or similar name, or patients who attended the same clinic, ward, etc.

f) If staff come across misfiled papers they must bring this to their manager's attention; and/or make arrangements for information to be re-filed in the correct chart. Staff should not assume that someone else will pick up on a misfiling error.

g) Case note tracking must always be updated to accurately reflect the location of the chart and ensure it can be easily found when needed for patient/client care or to meet the Trust's other legal responsibilities.

h) All documents 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.

i) 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 facilities or 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. It is not sufficient to simply write the name of the facility, ward or department only, as this will not guarantee safe and secure delivery to the correct address or recipient. A 'return to sender' address (if undelivered) should be clearly marked on the reverse of the envelope/package.

j) 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.

k) 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.*

l) 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 or personal phone number, without assuring yourself of the caller's right to that information.

m) 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.

n) 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.

o) 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.

p) 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.

q) 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.

r) 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.

s) 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.

t) Staff should follow the Trust's Email Policy and Electronic Transmissions Protocol when sending confidential information by fax or email.

u) Confidential / personal identifiable information about patients, clients or Trust employees should not be emailed to or from any staff member's personal (home) email account; and should not be stored or processed on any staff member's personal computer.

v) 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 (App1. 2.12).

w) Information sheets such as 'handover notes' used by staff working with inpatients should not be taken home and should be confidentially destroyed when no longer needed.

x) Staff diaries and portable electronic devices containing personal information should be kept secure at all times.

y) Personal identifiable information (letters, reports, etc.) sent to a shared printer should always be checked to ensure it is not mixed up with information printed separately or by other staff. Refer to the guidelines available on the Staff West site for use of pin & print capabilities when sharing Multi-Function Printers (MFP's).

z) Staff should never post confidential information or any inappropriate comments about patient, clients or other employees on social networking sites, including Text Messaging Services / Apps.

aa) Staff should always follow good record keeping practices, in accordance with the Trust's Records Management Policy and procedures, DHSSPS guidelines (Good Management Good Records) and their own Professional standards and practice.

REMEMBER: All individuals 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.

Western Health and Social Care Trust

Principles Governing Information Sharing[1] — Appendix 6

Code of Practice 8 Good Practice Principles[2]	GDPR Principles[4]	Caldicott Principles[3]
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. **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. **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. **4.** 'Third Party' organisations seeking information other than for direct care should be seeking anonymised or pseudonymised data. **5.** Any proposed use must be of clear general good or of benefit to service users. **6.** Organisations should not collect secondary data on service users who opt out by specifically refusing consent. **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. **8.** To assist the process of pseudonymisation, the Health and Care Number should be used wherever possible.	**a)** processed lawfully, fairly and in a transparent manner **b)** Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **c)** Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **d)** Data Quality - accurate and, where necessary, kept up to date **e)** Storage Limitation - kept for no longer than is necessary. **f)** Integrity and Confidentiality - processed in a manner that ensures appropriate security of the personal data Accountability is central to GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator (ICO). Principles relating to individuals' rights and overseas transfers of personal data are specifically addressed in separate GDPR articles.	**1.** Justify the purpose(s) for using confidential information. **2.** Only use it when absolutely necessary. **3.** Use the minimum that is required. **4.** Access should be on a strict need-to-know basis. **5.** Everyone must understand his or her responsibilities. **6.** Understand and comply with the law. **7.** The duty to share information can be as important as the duty to protect patient confidentiality

[1] These principles must be followed by health and social care organisations when considering use and disclosure of service user information.
[2] Code of Practice, paragraph 3.17.
[3] PDG Principles are adopted from the Caldicott Principles (revised September 2013) established in England and Wales.
[4] General Data Protection Regulation (GDPR) Principles apply from 25th May 2018 replacing the Data Protection Act 1998

The Caldicott Principles - Revised September 2013

Principle 1. Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.