Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM7
Issue number: 13

Code of Confidentiality Policy

Lead executive	Medical Director & Caldicott Guardian
Authors details	Information Governance Lead/DPO

Type of document	Policy
Target audience	All CWP staff
Document purpose	Outlines the Data Protection Legislation and Caldicott Principles

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 13 December 2021
Implementation date	December 2021	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM1	ICT Acceptable Usage Policy (AUP)
IM2	Email management procedure
IM5	Information asset register policy
IM6	Information sharing over arching policy
IM10	Information governance policy
CP3	Health records policy
CP40	Safeguarding children policy
CP63	Access to health records policy
GR12	Media policy
GR17	Freedom of Information policy
GR41	Corporate records policy
HR3.3	Disciplinary policy and procedure
HR13	Registration authority policy

Document change history	
What is different?	Updated external references 2.8 Access to information on mobile phones 2.9 Updated UK adequacy agreement 2.12 Updated fax ban information 2.15 Added email global address list risk 2.16 Microsoft Teams Information Governance Guidance 2.17 Principles of safe video consultation in Cheshire and Wirral Partnership NHS Trust Appendix 1 update sample police DPA form
Appendices / electronic forms	Not applicable
What is the impact of change?	Not applicable

Training requirements	Select - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	None

Financial resource implications	None

External references
1. Confidentiality: NHS Code of Practice NHS_Code_of_Practice.pdf 2. Patient leaflets www.cwp.nhs.uk 3. Information Commissioner's Data Protection, Freedom of Information and environmental information regulations 4. Caldicott 2 review to share or not to share 5. Information Commissioner's Data Sharing Code of Practice 2020 6. NHSx IG portal 7. NHSx **Records Management Code of Practice 2021.**

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
Not applicable		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	N/A	

Contents

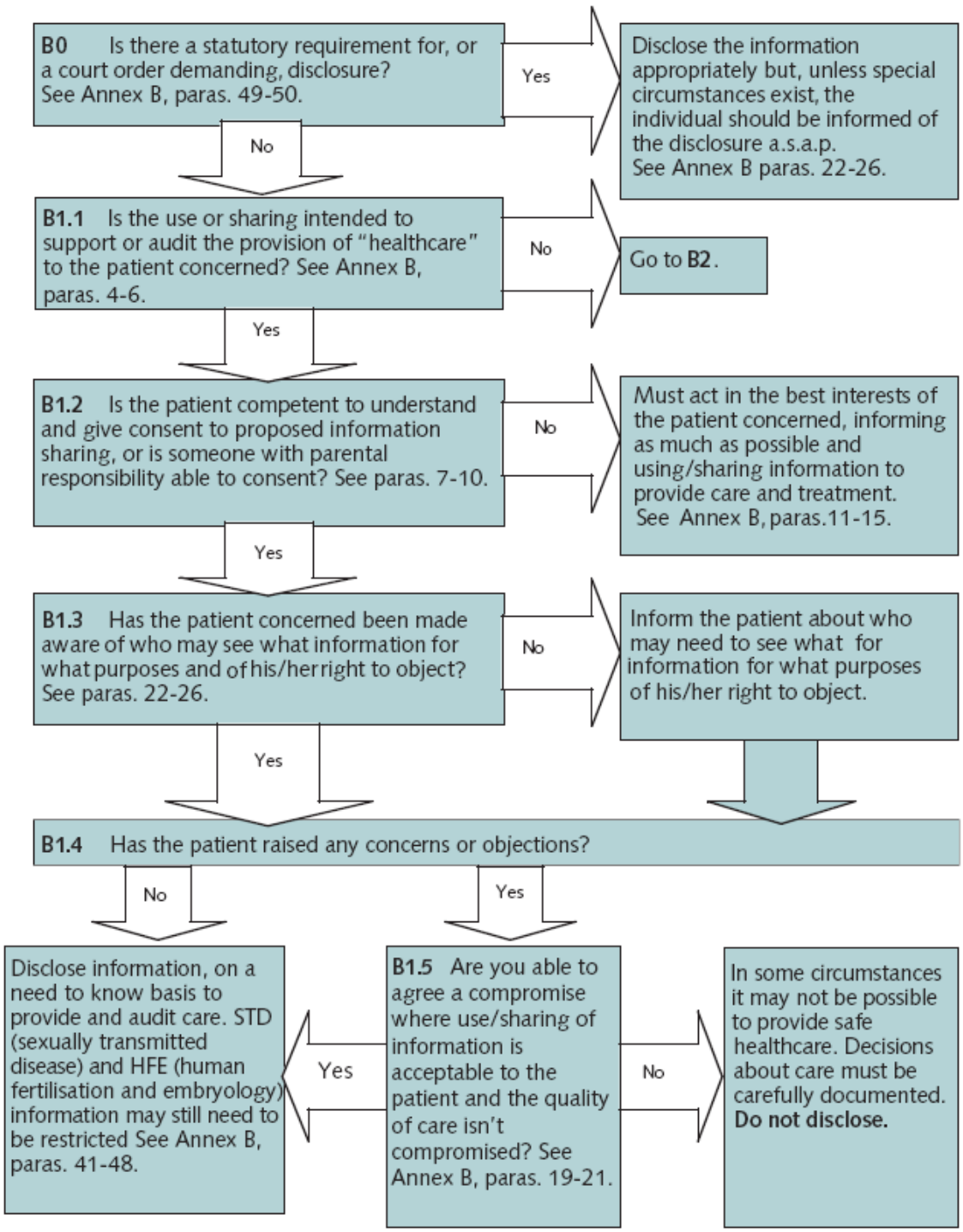
Quick reference flow charts for disclosure of information		4
1.	Introduction	8
2.	What is confidential information?	8
2.1	Disclosing and using identifiable information	9
2.2	Consent to disclosing patient and third party information	9
2.3	Members of the public recording staff	10
2.4	Caldicott	10
2.5	Subject access to information	12
2.6	What is Person Identifiable Information?	12
2.7	Who is an unauthorised person?	13
2.8	Accessing personal information or images on an electronic device	13
2.9	Transfer of information	14
2.10	Physical and electronic security (general)	16
2.11	Texting guidance	17
2.12	Fax printer ribbon and film guidance	17
2.13	Use of Dictaphones	17
2.14	Safeguarding information on computers	17
2.15	Use of the Email system	18
2.16	Microsoft Teams Information Governance Guidance	18
2.17	Principles of safe video consultation in Cheshire and Wirral Partnership NHS Trust	19
2.18	Indiscreet conversations	23
2.19	Safe havens	23
2.20	Legal implications	24
2.21	Implied consent	25
2.22	Lack of capacity to consent to disclosure of information	25
2.23	Passing on information for children and young people	26
2.24	Victoria Climbie Guidance Note	26
2.25	Statutory restrictions for passing on information	27
2.26	Information sharing policy	27
2.27	Information sharing with carers	27
2.28	Breaches of Confidentiality/Lost Records	27
2.29	Use of electronic systems	28
2.30	Press and broadcasting	28
2.31	Passing on information in connection with serious crime	28
2.32	Supplying of information to the police	29
3.	Duties and responsibilities	30
3.1	Chief Executive	30
3.2	Caldicott Guardian	30
3.3	Senior Information Risk Owner (SIRO)	30
3.4	Records & Information Systems Group	31
3.5	Information Goveranance Lead (Data Protection Officer) / Caldicott Support Function	31
3.6	Local managers	31
3.7	PALS officer	31
3.8	All staff	31

Appendix 1 - Requests for patient information by the Police	33
Appendix 2 - Consent to share health records with police	35
Appendix 3 - Simple patient consent to share reports	39
Appendix 4 - Consent to pass on contact details to other families	40

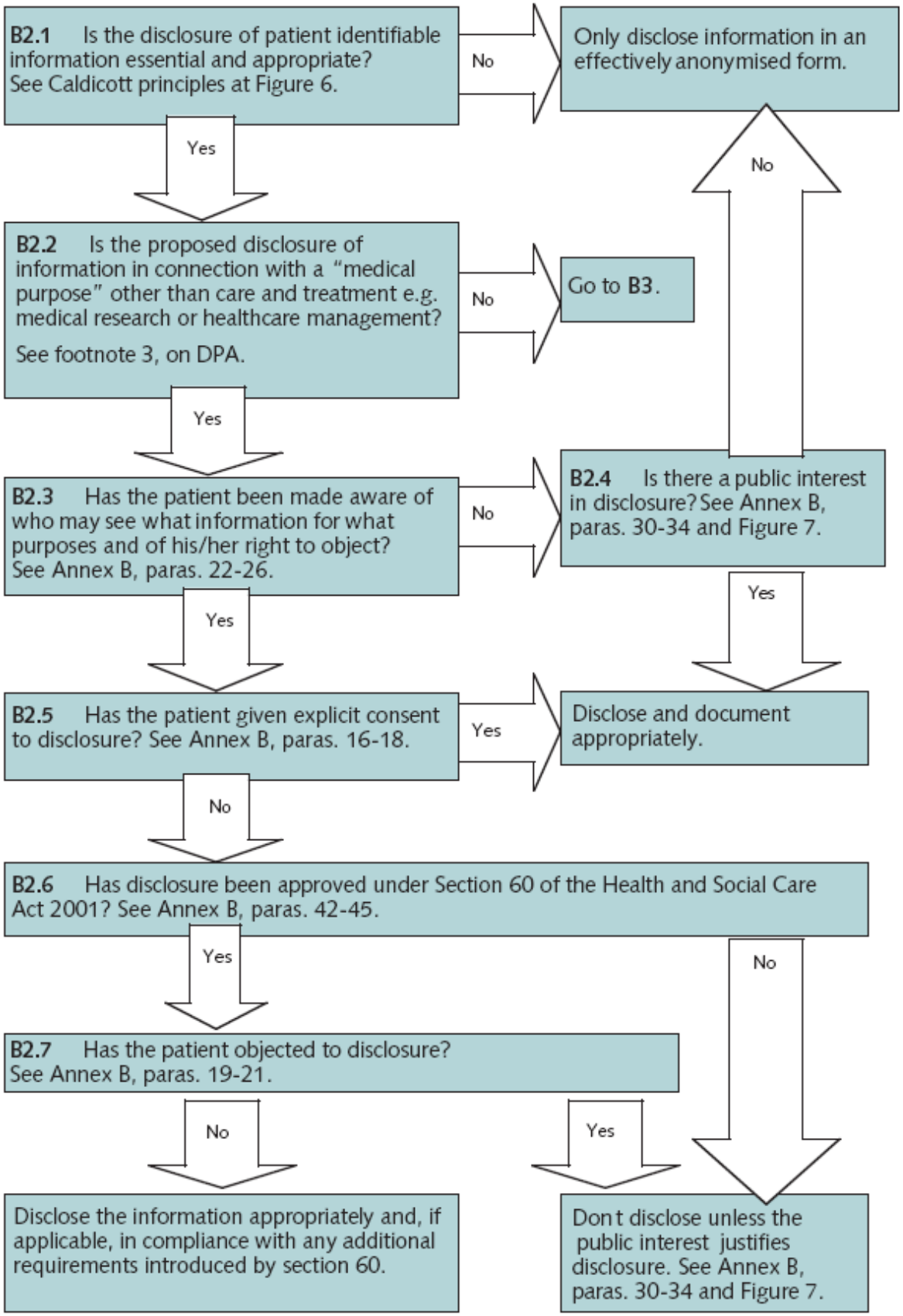
Quick reference flowchart
For quick reference the guide below is a summary of actions required.

Confidentiality: NHS code of practice
The flowcharts on the following pages have been taken from the `Confidentiality: NHS Code of Practice' document. Please see full code of practice for further guidance (website address given in references on page 1). Please note, the disclosure models are unaffected by the General Data Protection Regulation 2016 (GDPR) & the Data Protection Act 2018 (DPA18).

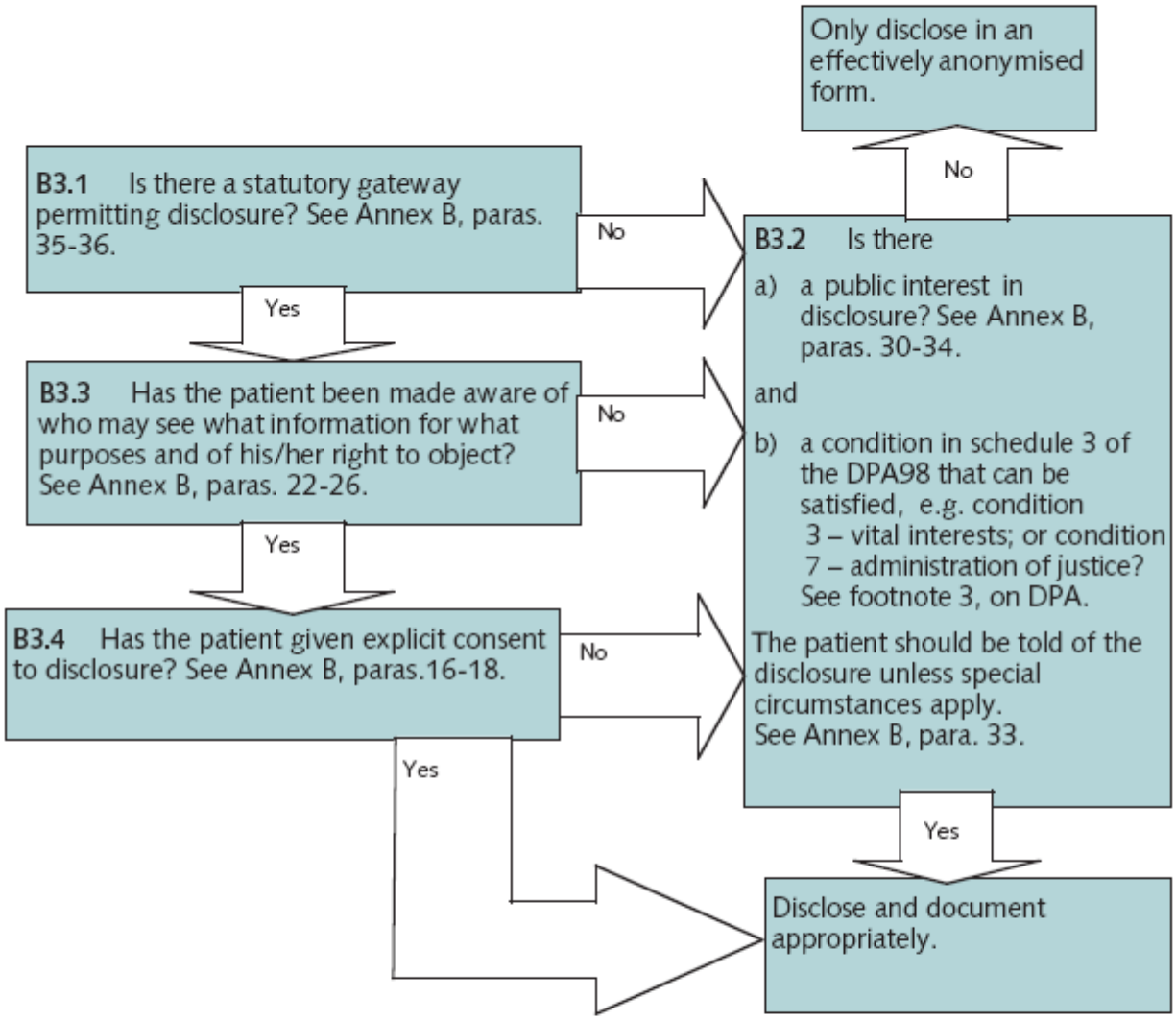
B1: Disclosure Model[11] – where it is proposed to share confidential information in order to provide healthcare



B2: Disclosure Model – where the purpose isn't healthcare but it is a medical purpose as defined in the legislation



B3: Disclosure Model – where the purpose is unrelated to healthcare or another medical purpose



When consent to share information is needed (non-care purposes)
Where an organisation wishes to use or disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

- Housing departments;
- Education services;
- Voluntary services;
- Sure Start teams;
- The police;
- Government departments.

Examples of where consent to share information is needed (non-care purposes)

Checking quality of care
- Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use; - Care audit activity on site; - Supporting Care Quality Commission audit studies; - Comparative performance analysis across clinical networks; and - Ensuring the needs of service users within special groups are being met e.g. children at risk, chronically sick, frail and elderly.
Protecting the health of the general public
- Drug surveillance (pharmacovigilance) and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency; - Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events; - Vaccine safety reviews; - Safety monitoring of devices used in healthcare; - Linking with existing National Registries for diseases / conditions; - Analysis of outcomes following certain health interventions (i.e. public health interventions as well as treatments); - Monitoring the incidence of ill health and identifying associated risk factors; - Identifying groups of patients most at risk of a condition that could benefit from targeted treatment or other intervention.
Managing care services
- Capacity and demand planning; - Commissioning; - Data for Standards and Performance Monitoring; - National Service Frameworks; - Clinical indicators; - Information to support the work of the Care Quality Commission; - Evidence to support the work of the National Institute for Health and Clinical Excellence; - Measuring and monitoring waiting times, in support of the 18 week target; - Data to support Productivity Initiatives; - Agenda for Change; - Benchmarking.
Supporting research
- Assessing the feasibility of specific clinical trials designed to test the safety and / or effectiveness and / or cost-effectiveness of healthcare interventions; - Identification of potential participants in specific clinical trials, to seek their consent; - Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research; - Providing specific datasets for defined approved research projects.

1. Introduction

There are several useful sources of guidance available nationally. NHSx have created a new Information Governance Portal which contains guidance for the public, health and social care front line staff and information governance professionals.

Staff should also refer to the Staff Information Governance Hand Book

The Code of Confidentiality Policy aims to clarify the principles that govern all use of personal identifiable information and to ensure that certain practices are adhered to. None of these practices are onerous and they should already be in every day use.

It should be noted that this is a generic Code of Confidentiality Policy for all staff and covers personal information concerning staff as well as people who use Trust services.

The health service holds large amounts of confidential information about you, members of your family, friends and colleagues; but the vast majority of this information will be about strangers, most of whom you are unlikely to meet. The information belongs to them and we are merely the custodians. Their information should be treated with as much respect and integrity as you would like others to treat your own information. Handle with care, it is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that personal identifiable information is not made available to unauthorised persons.

All staff should meet the standards outlined in this document, as well as their terms of employment (or other engagement agreements). Much of what is required builds on existing best practice. Everyone should make every effort to meet these standards and improve practice.

If staff are constrained from meeting these standards where appropriate organisational systems and processes are not yet in place, staff must inform their line managers of any specific problems or barriers that have been noted.

2. What is confidential information?

People who use Trust services entrust us with sensitive information relating to their health and other matters as part of seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. If service users lack capacity, this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Everyone who works for the NHS has a common law duty of confidence.

Information that can identify individuals must not be used or disclosed for purposes other than healthcare without:

- Explicit consent;
- Some other legal basis;
- Where there is a robust public interest or legal justification to do so.

In contrast, anonymised information is not confidential and may be used with relatively few constraints.

Identifiable information is generally held under legal and ethical obligations of confidentiality and it should not be used or disclosed in a form that might identify the data subject without their consent. However, there are a number of important exceptions to this rule and further guidance can be found in confidentiality guides which can be found in the references of this document.

2.1 Disclosing and using identifiable information

Many current uses of confidential information do not contribute to or support the healthcare that is directly received. Very often, these other uses are extremely important and provide benefits to society, e.g. medical research, protecting the health of the public and health service management and financial audit.
However, they are not directly associated with the healthcare that is received and we cannot assume that those who seek healthcare are content for their information to be used in these ways.

It is also extremely important that people who use Trust services are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, clinical governance and clinical audits, which are essential components of healthcare provision, might not be obvious to them and should be drawn to their attention. Similarly, whilst they may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important when the disclosure extends to non-NHS bodies.

Information may be released in cases where there is a danger to the data subject or others. If you receive a request from another agency or the police, etc, you should seek advice from your manager / Caldicott Guardian.

Ensure that you are familiar with the patient information leaflet Protecting and sharing information about you privacy notice Admin staff and clinicians should proactively ensure that people who use Trust services receive a copy of the leaflet at their first point of contact. It should not be left to chance that the leaflet has been seen in reception areas and noted. It should be recorded in patient records that information sharing issues have been discussed. There are also appropriate leaflets for Learning Disabilities Patients

2.2 Consent to disclosing patient and third party information

People who use Trust services generally have the right to object to the use and disclosure of confidential information that identifies them and they need to be made aware of this right. Sometimes, if they choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited or that it is not possible to offer certain treatment options. Their wishes must be confirmed and recorded in their health record. Staff should verify personal details with them so that the Trust has complete and accurate up to date information.

There are situations where consent cannot be obtained for the use of disclosure of confidential information, yet the public good of this use outweighs issues of privacy. Section 251 of the NHS Act 2006 currently provides an interim power to ensure that identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without consent.

Rule
When releasing information to either the patient or their representative, third party information must not be disclosed.

Definition
Third party information is anyone other than the patient or health & social care professionals working within the Trust i.e. staff names of those working in the Trust are not removed.

Standard
When trying to ascertain if an entry in the records should be disclosed apply the following:

If the third person could be identified from the entry, or information has been provided by a third party –do not dislcose.

Examples
'The patient has had a visitor this afternoon' – do not remove, third party not named and cannot be identified.

'The patient's son, John, has visited this afternoon' – remove 'son, John' – can be identified from this entry.

'The patient's eldest son has visited this afternoon' – remove 'eldest son' – can be identified from this entry.

'Telephone call received from patient's mother (then the content of the phone call is recorded) – remove the whole entry as we do not have permission from the patient's mother to disclose this information

Guidance
In many cases it will be a 'judgement call'. If unsure please consult with the Trusts' Information Governance Lead/DPO.

Information from other organisations
If there are copies of records from other organisations within the records and it is felt that these should be released, then these should not be released without liaising with the other organisation to check if there are any concerns. If the other organisation is not contacted because release by the Trust is not felt necessary and the patient later queries the omission, the applicant should be directed to approach the other organisation for access to this information.

2.3 Members of the public recording staff

There are occasions when members of the public will wish to record staff on the telephone, on Trust property or in public/person's home. There are no legal grounds to prevent this from happening. Article 8 of the Human Right Act 1998 would prevent staff from recording patients and it would be a breach of data protection laws for staff to record patients without consent. If a staff member is made aware that a patient is recording a conversation/ consultation etc., they should have a discussion with the patient/ member of public in order to understand why they are recording the interaction, as this may be due to poor memory. In this instance, the staff member should advise the patient's carer that the medical information recorded is confidential and should not be published. If the member of the public is going to publish the recordings, for example to a solicitor, the Trust needs to be made aware. The Trust will then have the opportunity to make representations. If a staff member is made aware that they are being recorded, they should seek to understand why the member of the public wishes to record the interaction and to remain professional during the interaction.

2.4 Caldicott

'*The Caldicott Committee: Report on the Review of Patient-identifiable Information'*, was published in December 1997, and the resulting conclusions in the report formed the basis for changes in the way we protect personal information. The guidelines resulting from the Caldicott report have now been built into the Information Governance framework.
The Report made sixteen recommendations and one of the key recommendations was the appointment of a Caldicott Guardian for each organisation. All NHS organisations have a Caldicott Guardian who is responsible for agreeing and reviewing protocols that govern the disclosure of personal identifiable information across organisational boundaries.

The Committee also developed a set of 6 general principles for the safe handling of personal identifiable information and these Principles are the guidelines to which the NHS works to help comply with the Data Protection Legislation. The principles cover information held in whatever format – whether electronically, paper, verbal, or visual.

There have been two further reviews of the principles resulting in two additional principles.

The 8 Caldicott principles for handling personal identifiable information

Justify the purpose
Every proposed use or transfer of personal identifiable information within or from another organisation should be clearly defined (and reviewed if continuing).

Do not use personal-identifiable information unless it is absolutely necessary
Personal identifiable information items should not be used unless there is no alternative.

Use the minimum necessary personal-identifiable information
Where use of personal identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.

Access to personal identifiable information should be restricted on a strict need-to-know basis
Only those individuals who need access to personal identifiable information should have access to it, and they should only have access to the information items they need to see.

Everyone should be aware of their responsibilities
Action should be taken to ensure that all staff are aware of their responsibilities and obligation to respect personal confidentiality.

Understand and comply with the law
Every use of personal identifiable information must be lawful.

Duty to share
The duty to share information can be as important as the duty to protect confidentiality.

Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

General Data Protection Regulation 2016 (GDPR)

First Principle	Personal data shall be processed fairly and lawfully and with transparency 'lawfulness, fairness and transparency'
Second Principle	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 'purpose limitation'
Third Principle	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 'data minimisation'
Fourth Principle	Personal data shall be accurate and, where necessary, kept up to date. 'accuracy'
Fifth Principle	Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes. 'storage limitation'
Sixth Principle	Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 'integrity and confidentiality'

Data Protection Registration
The Trust holds a Data Protection Registration which enables the Trust to hold personal identifiable information in hard copy or electronic format. Staff who carry confidential information outside Trust premises must ensure that the information is secure at all times. This will include lap top computers, palm tops, memory sticks and information received on home computers. In accordance with principle two of GDPR, personal data shall be collected for specified, explicit and legitimate purposes and not

further processed in a manner that is incompatible with those purposes. 'purpose limitation' (e.g. for business or research purposes) without the permission of the data subject.
The Trust is registered to transfer information worldwide. If transferring information outside the UK, the Data Protection Officer (Information Governance Lead/DPO) must be advised to ensure that Data Protection (GDPR) requirements will be met.

2.5 Subject access to information

Data Protection legislation safeguards the processing of personal information.

Individuals have the rights of subject access – this means:

- Individuals have a right to find out what information is held about them on computer and in some paper records;
- Individuals have the right to have inaccurate personal information rectified, blocked, erased or destroyed. If they think they have suffered damage or damage and distress as a result of the processing of inaccurate data, they have the right to apply to a court;
- Individuals have the right to request in writing that a data controller does not use their information for direct marketing by post, fax or email (GDPR requires that individuals must give explicit consent for direct marketing);
- Individuals can write to a data controller to ask that they do not make any decisions that significantly affect them based solely on an automated process. Where a decision has already been taken they can ask the data controller to reconsider or to use a different method to make the decision (GDPR gives individuals the right to object to automated decision making);
- If they think this will or is likely to cause them or someone else substantial damage or distress they can ask that data controller to stop that processing.

They are allowed by law to see their medical or personnel records under GDPR. There is a duty to keep medical records up to date. If they feel anything has been added to the record that is factually incorrect, they have the right to have it amended or deleted, see Access to Health Records Policy

Can any of the information held in the record be withheld?
Yes, information contained in records likely to cause harm to mental or physical state, or that of other people, may be withheld. Any third party information would not be revealed without their consent.

Similarly, if they wish to see employment information, they should ask the Human Resources department, see Corporate Records Policy

2.6 What is Person Identifiable Information?

The Caldicott Committee concluded all items of information which relate to an attribute of an individual should be treated as potentially capable of identifying persons and hence should be appropriately protected to safeguard confidentiality.

These items include:

- ⦿ Surname
- ⦿ Forename
- ⦿ Initials
- ⦿ Address
- ⦿ Postcode
- ⦿ Sex
- ⦿ NI number
- ⦿ NHS Number
- ⦿ Ethnic group
- ⦿ Date of birth
- ⦿ Other dates, e.g. death, diagnosis
- ⦿ Occupation
- ⦿ Local identifier, e.g. hospital or GP Practice number

2.7 Who is an unauthorised person?

An unauthorised person is anyone who does not need to know the information. Your job role, or level of access to a computer system, provides you with a level of authority to access information. Do not assume that all of your work colleagues are authorised to see the same information that you are. It is important to remember this even if they are in a more senior role to yourself - if they do not need to know the information, they do not need to have it. If you are in doubt as to whether you should share the information with one of your colleagues, seek the advice of your manager, Caldicott Guardian, Information Governance lead or Caldicott Support Function.

In certain instances, an NHS body or member of staff may have a statutory responsibility to pass on patient information.

The NHS has a statutory obligation to notify the government of certain infectious diseases for public health purposes, e.g. measles, mumps, meningitis, tuberculosis, but not HIV / AIDS. Births and deaths must also be notified.

A court of law can insist that medical information be disclosed to them. The process for this will be undertaken by a senior manager. Always obtain advice from your manager under these circumstances.

Solicitors sometimes request medical reports but these requests must be accompanied by the signed consent of the patient. Any third party information in the record will be withheld unless the third party has also given written consent. When in doubt seek advice from your manager as before.

Limited information is shared with Clinical Commissioning Groups (CCG) and other NHS organisations to assist with the organisation of national public health programmes.

Do not access patient information for anything other than your official duties, as misuse of any system used for recording information in confidence will result in disciplinary action. See Disciplinary Policy and Procedure It is not acceptable for staff to access either their own records, or to access the records of relatives, friends, or neighbours.

This policy is against this inappropriate use of any system used to record personal information. Staff and patients have a right to be told what information is held about them in their health and employment records, but this should only be done in accordance with Data Protection Legislation. Patients may contact PALS for appropriate sign posting:

Organisation	Contact	Contact Number
Cheshire and Wirral Partnership NHS Foundation Trust	Patient Advice Liaison Service (PALS)	0800 195 4462

2.8 Accessing personal information or images on an electronic device

Accessing an individual's personal information which may be contained in their electronic mobile device or phone is protected under the Data Protection Act (2018). All images and information contained on these devices is legally owned by the insividual and should not be accessed without the owners permission or through a legal process i.e. Police warrant. Any attempt to access an individual's personal information or images without permission or through a legal process may be deemed a breach of Data Protection Principles. However the circumstances of each situation may be different and should be assessed under the framework of reasonableness, proportionality and necessity. If immediate access to personal information or images is required due to an emergency or critical situation this should be only be conducted in consultation with the Responsible Clinician (if the device belongs to a patient), Police and senior management team. **If the phone/electronic device is deemed or suspected to contain "Indecent Images of Children" (IOC), staff members should not attempt to access the device, this should be immediately directed to the Police and senior managers for support.** All decision making should be fully recorded into the patients care record or staff record in the case of a member of staff, and Datix incident form complete. The individual should

be informed of any decision to access their personal information or images at the earliest opportunity and advised of the decision pathway.

2.9 Transfer of information

Follow any established information sharing protocols or agreements (ISPs / ISAs) e.g. Information Sharing Policy Staff should work within these protocols where they exist and within the spirit of this policy where they are absent.

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information. Impersonators may try to get information sent to them i.e. paper copies in the post and they may also telephone the Trust posing as the patient or as a professional e.g. General Practitioner.

If staff suspect attempted identity fraud they must inform their line manager and the Data Protection Officer and also complete an online Datix Incident Form

The transfer of personal identifiable information, by whatever means, can be as simple as:

- Taking a document and giving it to a colleague;
- Making a telephone call;
- Sending a fax (secure email should be used instead of fax where possible);
- Passing information held on computer.

In all cases, however simple or complicated, the Caldicott Principles must be adhered to, in order to ensure that personal identifiable information is not disclosed inappropriately.

Always remember that you are responsible for the safe keeping of confidential information once it has been passed to you.

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be. Share the minimum necessary to provide safe care or satisfy other purposes.

When transferring paper notes that contain personal identifiable information, ensure CONFIDENTIAL is marked in a prominent place on the front of the envelope. Make sure that the address of the recipient is correct and clearly stated, using the following format:

- Name;
- Designation (job title);
- Department;
- Organisational address;
- Write a return address on the back of the envelope (if using a plain envelope).

If patient-identifiable information is to be sent in carrier (internal) envelopes, the envelope must be sealed and marked CONFIDENTIAL. Internal mail should still be properly named and addressed, for example, not just to “Dave at Denton”. Depending upon circumstances, it may be more appropriate and expedient to transport the information personally. If this is the preferred option, do not leave any information inside an empty car during transit, and make sure that it is locked away securely in the boot.

It is not appropriate for unpackaged information to be given to a colleague for delivery. If you have any specific questions regarding transferring patient records, contact your line manager for further guidance.

Transfers outside United Kingdom

The European Economic Area (EEA) is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway. The current EU member states are in Table 1.

Table 1: The European Union Member States				
Austria	Belgium	Bulgaria	Croatia	Cyprus
Czech Republic	Denmark	Estonia	Finland	France
Germany	Greece	Hungary	Ireland	Italy
Latvia	Lithuania	Luxembourg	Malta	Netherlands
Poland	Portugal	Romania	Slovakia	Slovenia
Spain	Sweden			

Further details can be found on the EEA website

An Adequate Level of Protection

1. The European Commission has the power to determine whether a third country (i.e. not an EU member state or an EFTA country) ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into.
2. The Commission has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, the US Department of Commerce's 'Safe Harbour' Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.
3. Information on countries with an adequate level of protection and the US Privacy Shield (formerly Safe Harbor) agreements can be found within the European Commission decisions on the adequacy of the protection of personal data in third countries
4. To ensure compliance, if information is to be transferred to a country not listed in Table 1 above, it should check the website referred to in paragraph 3 to obtain up to date information about whether the country is deemed to have adequate protection.
5. If the transfer is to a country not on the adequacy list, measures should be put in place to ensure that there is an adequate level of protection when person identifiable information is transferred. This requires that contractual agreements are drawn up specifying the terms on which the information is transferred and the restrictions on its use for further purposes.
6. All risks to the information should be assessed and put protective measures in place to reduce any risks. Potential risk areas to be taken into account include:
    - What information is being transferred?
    - Have the data subjects been informed?
    - To what country is the information being transferred?
    - What are the purposes of the transfer?
    - What data protection laws are in place in the overseas country?
    - Is data protection appropriately covered in the contractual arrangements between the organisations?
    - Is restriction on further use appropriately covered in the contractual arrangements between the organisations?
    - How is the information to be transferred?
    - What security measures are in place to protect the information during transfer?
    - What security measures are in place in the recipient organisation?

7. Further guidance is available from the Information Commissioner's Office. If transferring information outside the UK, the Data Protection Officer (Information Governance Lead/DPO) must be advised to ensure that Data Protection requirements will be met.
   Note: The Brexit withdrawal bill enshrines GDPR into UK law. The Data Protection Act 2018 (UK) relates to crime and taxation which GDPR does not include. As a third country (outside the EEA),

the UK has acquired an adequacy agreement and to be able to continue to transfer information within the EEA.

8. Organisations must also comply with the following guidelines issued by the Department of Health.
    - Decisions on whether to transfer person identifiable information must only be taken by a senior manager or senior care professional that has been authorised to take that decision;
    - Organisations will need to obtain an assurance statement from third parties that process the personal data of their service users or staff overseas. This assurance may be within the contract between the two organisations or within other terms of processing. The Trust uses the standard NHS contract which includes confidentiality clauses.

2.10 Physical and electronic security (general)

Room access – All staff have a responsibility for ensuring that all personal information is not left unattended. However, where this can be justified, consideration must be given to restricting room access. When undertaking Trust duties staff must always wear their identity badge and appropriately query the status of unknown persons within CWP premises. Staff must escalate to senior staff any concerns if anything suspicious or worrying is noted. Access controls/keys to CWP premises must not be disclosed or given to unauthorised personnel under any circumstance.

Where a room can be secured without compromising patient care (e.g. where the patient information is unlikely to be needed by non key-holders), then it must be locked. Each staff member has individual responsibility when leaving an area which contains confidential/sensitive information to shut and/or lock doors and cabinets as required. If any staff member loses any key or other access tool this must be reported to senior staff member and also onto CWP reporting system.

Work areas - identifiable, confidential information must always be held securely. In areas which cannot be secured due to environmental factors i.e. reception areas and which are accessed by a wide range of people (including possibly the public), such areas must never be left unattended and access to information must be secured immediately on leaving. The Trust operates a clear desk policy. Where it is impractical for this to be achieved, access to the work area must be restricted.

Wherever possible, staff must avoid taking confidential information away from your work premises unless this is necessary to carry out your duties. Where this applies staff have a duty to secure all sensitive information and not leave confidential information unattended or accessible to unauthorised persons in areas such as private homes or vehicles.

When disposing of confidential paper-based information, staff must ensure that it is shredded placed into designated waste bins and never put directly into a general waste paper bin. CWP has contracts with confidential waste shredding companies.

Personal notes, pocket books and work diaries containing personal identifiable information must be kept secure at all times. Where the information is no longer required, staff must ensure that this is disposed of appropriately through secure measures. Staff must return work diaries to their line manager if they no longer needed. Where the information is required for an on-going purpose, it should be locked securely away. Any loss of personal identifiable information must be reported immediately to a senior staff and recorded onto CWP reporting system.

Any staff member who is not the intended recipient of documents containing personal information must immediately forward these to the named person or where this is not known, seek advice from your manager, Care Group Caldicott Champion, Caldicott Support Function, Information Governance lead, or Caldicott Guardian. If you identify any document containing personal identifiable information, such as letters or results, staff must take reasonable measures to decrease the possibility of these being seen by inappropriate persons. All documents must be filed and locked away when not in use.

2.11 Texting guidance

It is appropriate to rely on implied consent for confidentiality purposes when contacting individual patients and service users about their individual care or requesting they complete a friends and family test survey. Explain to the patient or service user that it is their responsibility to keep and provide an up to date or mobile phone number, and to be clear that the service is not responsible for onwards use or transmission of a text message once it has been received by the patient /service user. When sending a text message:

- Minimise the amount of personal/confidential patient information you communicate via mobile messaging.
- Remember that mobile messaging conversations may be subject to freedom of information (FOI) requests or subject access requests (SARs).
- Do not allow anyone else to use your device.
- Set your device to require a passcode immediately, and for it to lock out after a short period of not being used.
- Disable message notifications on your device's lock-screen.
- Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book.
- Consider the possibility that someone else may read a text message that you send to a patient or service user, e.g. a family member accessing their unlocked mobile phone, or the phone being passed on, sold or stolen and ending up in the possession of someone else.
- Only the minimum amount of personal data for the purpose should be communicated via text.
- For further guidance visit the NHSx Information Govenance Portal: template-email-and-text-message-communications

2.12 Fax printer ribbon and film guidance

Fax Printer Ribbon or Film is the device consumable normally provided in 'refill roll' or 'refill cartridge' form designed to work with the relevant fax printer device. These function by the device 'thermal print head' melting a coating of ribbon or film onto the material that the print is applied. As a consequence of thermal printing a readable negative copy image of the printed document may be retained on the used portion of the ribbon or film. Used ribbons or films should therefore be disposed of via confidential waste.

Note: Since January 2019 NHS Trusts have been banned from purchasing new fax machines, following the Secretary of State for Health and Social Care ordering their complete phase-out by April 2020. They may now only be used to transfer PCD when absolutely necessary.

2.13 Use of Dictaphones

There may be occasions when staff wish to use a Dictaphone to record verbal information. It is essential, that any information recorded, in any format, is secure and not kept for longer than necessary. Dictaphones can be used provided that:

1. The Dictaphone containing clinical information does not leave Trust premises
2. The Dictaphone is deleted of all confidential clinical content when no longer needed
3. The Dictaphone is kept either with the employee at all times, or in a secure place whilst it holds clinical information.
4. The Employee adheres to the all the requirements of this policy and the Health Records Policy

Note: All staff are personally accountable for all information recorded and stored.

2.14 Safeguarding information on computers

The security and confidentiality of information held on computer must be maintained at all times.

Staff must never leave a computer unattended whilst accessing person identifiable/sensitive information. Staff must never leave personal identifiable information on screen unattended for unauthorised persons to view. Staff must ensure that all computers are logged off when no longer required. Failure to do this may lead to a breach of security and increase the risk of unauthorised access to personal information.

Individual staff will be held responsible for ensuring the security of personal log on codes and these must never be disclosed to others. Managers should not compromise a member of staff by asking for their password for convenience or any other reason. If it is absolutely necessary, (e.g. to access information when a person is in danger and the owner of the password cannot be found), contact the ICT Servicedesk.

All personal identifiable information must only be stored in secure network drives with appropriate permissions. Where information is required to be transported this should be via a Trust approved encrypted memory stick. Encrypted access codes to shared memory sticks must never be disclosed to unauthorised others. When the information held is no longer required the information must be removed from the memory stick. Further advice on the retention of information can be found in the NHSx **Records Management Code of Practice 2021**

Permissions to outlook calendar are set appropriately but are potentially viewable by all staff. Users who use diary systems e.g. Outlook calendar and enter Person Identifiable Data (PID) in to those systems, need to ensure that access permissions to those diaries are set so that only permitted staff have access to those details.
Windows users should remember that when deleting files they are moved to the "recycle bin". Therefore, the recycle bin should be emptied on a regular basis. If in doubt, check with the ICT Department.

Passwords are the keys that provide access to information and you MUST NOT disclose your password to ANYONE under any circumstances and never write your password down as, this could be seen by other users. Always change your password when prompted and the use of family or pet names or any other names are not recommended. Passwords should be a minimum of 8 characters and should be a mixture of letters and numbers, i.e. using 5 instead of S, 1 instead of I, etc. Passwords should be easy to remember and difficult to guess.

Managers should not compromise a member of staff by asking for their password for convenience or any other reason. If it is absolutely necessary, (e.g. to access information when a person is in danger and the owner of the password cannot be found), contact the ICT Servicedesk.

Your computer should be shut down at the end of the working day unless it is needed to work unattended, e.g. for print-outs.

Destruction and / or disposal of computers should be logged with the ICT Servicedesk and completed by an approved disposal company. Staff should not remove or relocate computers without first checking with the ICT Department.

Portable computers / removable media
Individual staff must not leave portable computers/removable media unattended in cars or other easily accessible areas. All portable equipment must be secured appropriately when not actually being used.

Always ensure that you:

- Have the authority to take equipment off-site;
- Have permission to transfer personal identifiable information off-site and that:
    - Your equipment is supplied and encrypted by the ICT Servicedesk;
    - You store backups securely and complete them regularly whilst using portables / removable media. Backups must only be made to Trust supplied encrypted memory sticks;
    - All equipment is locked away when not in use;
    - Every effort is taken to prevent loss or theft of your equipment.

2.15 Use of the Email system

Ensure that the contents are appropriate, legal and not offensive
You are responsible for the contents or your Emails. Ensure that the content is not sexually or racially offensive, or otherwise illegal.

What is sensitive information?
Sensitive information includes: Person-Identifiable Data (PID). Data protection legislation classifies sensitive information as:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs or trade union membership
- Processing of biometric or genetic data
- Health data
- Sexual orientation or sex life

This can refer to a service user, carer, visitor, staff member, foundation trust member, supplier and contractors etc - Commercially sensitive information.

This could include information on contract prices, business plans etc.
Sensitive information should be sent by the most secure route possible.

Patient Identifiable Data (PID) should only be exchanged electronically when encrypted. NHSmail email sent to secure domains it automatically encrypted and complies with the pan-government secure email standard. NHSmail is accredited to the Health and Social Care secure email standard and is suitable for sharing patient identifiable and sensitive information.

When sending emails outside of NHSmail, use [secure] at the start of the email subject. [Secure] is not case sensitive. **Note:** brackets must be square brackets or the message will not be encrypted. `Secure' is not case sensitive. The NHSmail service will assess whether encryption is required.

- If the domain the email is being sent to is accredited, the email will be sent securely and no further encryption is required.
- If the domain the email is being sent to is not accredited, and therefore insecure, the NHSmail service will programmatically enforce the use of the ecryption tool to protect the email data. The recipient will need to log into the Trend Encryption Micro portal to unencrypt the email before it can be read.

NHSmail works with the Government Digital Service (GDS) to regularly update the list of accredited domains.

How to send an encrypted message from nhsmail:

- Send the recipient the recipient Accessing Encrypted Emails Guide so they can register for the service.
- Once the recipient of the information has registered for the encryption service and confirmed to the sender that this is complete, confidential information may be sent to the recipient using [Secure] at the beginning of the subject field of the email.
- Send the message.

The service will then encrypt the message and deliver it to the intended recipient. The sent item will be stored unencrypted in your sent items folder, any replies received will be decrypted and displayed as normal in NHSmail.

What is the CWP policy on secure email?

- Communication with patients, relatives and carers should be by email rather than traditional postal methods (if requested);
- Emails containing sensitive information should be sent to the minimum number of addresses;
- Staff should only forward or "reply to all" sensitive information where necessary;
- Person-identifiable information must be anonymised wherever possible and names must NOT be used in the subject field (the title of the email);

- Staff should ensure that they are aware of and follow the following policies when dealing with sensitive information: See Information Governance Policy & ICT Policy

What else do I need to consider?
There are some other email functions that staff need to consider. Staff should ensure that the address list within their email is set to CWP staff rather than the global (national) address list. If the default address list is used it is easy to select a member of staff with the same name who works for a different organisation which may result in a breach.

Email accounts with automatic forwarding, which might automatically send emails to a non-secure address, will no longer be supported.

A guide for sending and receiving encrypted emails from cwp mail accounts can be found on the information governance page on the intranet.

DO NOT disclose your email password to **ANYONE,** and remember to ensure you either log out of the system or lock your computer (by pressing CTRL-ALT-DELETE then selecting 'Lock Computer') when you leave your computer to avoid emails being sent out in your name or sensitive information being inappropriately accessed.

Always remember that the information contained in emails may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of Emails and any replies cannot be guaranteed.

2.16 Microsoft Teams Information Governance Guidance

Background
Information Governance concerns have been raised in relation to the recording of Microsoft Teams meetings and the use of the chat function.

MS Teams Recordings & Live Transcript
The use of MS Teams recordings or transcripts for clinical or HR meetings purposes is not permitted as they will have to be disclosed if requested as part of a Freedom of Information Request (FOI) or Subject Access Request (SAR).

Recording general meetings as a video or a transcript is permitted for the purpose of minute taking.

Explicitly state to all present what the purpose is and that the recording or transcript will not be retained as the minutes will act as the formal record of the meeting. Consent is not required.

The recording or transcript should only be downloaded for the purpose of completing minutes and should be deleted when they are complete. Follow the links for further information and guidance on downloading and deleting recordings in MS Teams.

If someone in attendance at the meeting starts to record the meeting, the host will receive an immediate notification and they should stop the recording.

Microsoft Teams - Person Identifiable Information
Do not use the chat function for any personally identifiable information.
Any message sent via the chat function is retained on Teams and will be considered a record, and therefore, subject to Subject Access Requests (SAR) and Freedom of Information Requests (FOI). If anything is added in error, it can be deleted from the chat but the chat thread itself cannot be deleted.

Microsoft Forms - Person Identifiable Information
Microsoft Forms is a simple to use application that is part of Office 365 for creating surveys, quizzes and polls. It enables users to quickly create a form, collect responses and produce automated visuals e.g. charts.

Do not use MS Forms for collecting data containing any sensitive personally identifiable information.

Staff should undertake the specific Caldicott/Information Governance and Microsoft 0365/MS Teams & Forms training session prior to using MS Forms.

Staff use of MS Forms will need manager approval via ICT service desk.

Staff should not use any `off the shelf'/free to use downloadable products, such as Google Forms or the free online version of SurveyMonkey, as they frequently do not comply with Information Governance requirements.

2.17 Principles of safe video consultation in Cheshire and Wirral Partnership NHS Trust

General information
The decision to offer a video consultation should be based on the patients need, clinical prioritisation and clinical judgement. There is no need to use video when a telephone call is sufficient. Be aware that patients or their relatives may record the video consultation.
The platforms that will be used to undertake video consultation are
1) Accurx Fleming for one to one patient consultations (link to user guide)

2) Microsoft Teams for video conferencing , group therapy, MDTs, CPAs, Seclusion Reviews (link to user guide)

3) WEBEX for video conferencing, MDTs, CPAs, Seclusion Reviews (link to user guide)

Practitioners are strictly advised against using other technology platforms (e.g. Zoom, Face-time, WhatsApp) as the privacy and security of these platforms cannot be assured.
If you are working from home and using your own equipment, check your internet access is secure (e.g. use a virtual private network Cisco Anyconnect and avoid public Wi-Fi), and make sure any security features are in use.
During COVID-19, you can use your own devices to support video conferencing for consultations, mobile messaging and home working where there is no practical alternative. Reasonable steps to ensure using your own devices is safe include setting a strong password, using secure channels to communicate, e.g. tools/apps that use encryption, and not storing personal/confidential patient information on the device.

Information governance
The Trust has undertaken data protection impact assessments (DPIA) for the following platforms: Accurx Fleming, Microsoft teams and WebEx.

Safeguard patients' personal/confidential information in the same way you would with any other consultation.

The consent of the patient is implied by them accepting the invitation and entering the video consultation. It is good practice to confirm and record their consent for a video consultation and confirm whether the consultation is being audio or video recorded. If an adult lacks capacity, you must obtain consent from someone with authority to act on their behalf for healthcare decisions and/or proceed with the consultation on the basis that it is the patient's best interests to do so.
If the Microsoft Teams platform is being used (especially in the case of Group Therapy), it is possible that participants are able to record the video conference. This only appears to be an option if the participant holds an NHS.net (internal) email. If they do begin to record, the host will receive an

immediate notification and they are able to stop the recording. During group therapy, the advice would be that this should not be recorded unless consent had been gained from all involved on the call. Young people under 16 should be assessed by phone or video if consulting remotely to assess capacity and safety.

• If the child does have the capacity to consent to a phone or video consultation, then confirm whether they would they like another person (for example, parent or family member) present on the call or not.
• If a competent child wishes to discuss a matter in the absence of a parent, all the usual principles apply in relation to confidentiality (GMC guidance).
• Consider the voice of the child, even if children are unable to legally consent to an examination, ask the child if it is acceptable first, they should have as much involvement and say in their care as possible.
• An opportunity to speak to adolescents alone may be more difficult if they are at home. Consider how you will still have these vital conversations.

For children who do not have capacity to consent, then consent would need to be sought from someone who has parental responsibility (or delegated parental responsibility), unless it is not in the child's best interest. Apply the same principles used in face-to-face practice.
Document the name and relationship with the adult and/or person(s) present. If a child is the subject of the consultation make sure you see them and that you don't just talk to the adult(s).
Ask for consent if a trainee, interpreter, chaperone or a multidisciplinary team (MDT) member wants to join the consultation. During an examination, ask others to switch off their camera or leave the room if their presence is not appropriate or the patient does not consent.
It is essential that colleagues are still able to talk to each other and share appropriate information about the people in your care, including with social care. Where possible use the phone, secure NHSmail or MS Teams.

Identity
Confirm the patient's identity if they are not known to you, e.g. check name and date of birth. If you have safeguarding concerns, and the patient is unknown to you, verify their ID, e.g. vouching if you have access to the patient's clinical record, or by asking for photo ID.

Introduction
Introduce yourself and everyone else in the room, even those off camera and confirm with the patient that they (and you) are alone. Follow this with:
• checking if the patient or anyone else is recording the consultation
• ensuring you use a private, well-lit room and ask the patient to do the same. You should safeguard personal/confidential patient information in the same way you would with any other consultation
• taking the patient's phone number in case the video link fails
If the connection or video quality is poor, ask the patient to re-book or conduct a phone or face to face consultation as it is possible you could miss something due to technical interference

Starting the examination
Setting up Your initial focus should be on the camera position in order that the patient sees your full face and you are in focus. Confirm the patient's location in case you need to send help: they may not be at their home address. Then explain the nature and extent of the examination and seek verbal consent. When talking, look at the camera. When listening continue to look at the camera and screen. Signpost what you are doing when you need to look away to avoid looking uninterested.

Safety netting
Be particularly careful to summarise key points and explain next steps in language that will be clear to the patient:
• Explicitly check understanding.
• Provide clear safety netting instructions.
• Actively signpost for support, e.g. to social prescribing link workers.

Documentation
Make contemporaneous written records in the patient's medical records, as you would in a standard consultation. Do not record the video or audio of the consultation unless there is a specific reason to do so, and there is explicit and informed consent from the patient, document these discussions and decisions in the clinical record. The process of obtaining and documenting consent should include explaining why a recording will help in providing clinical care, who can access the recording, where and how it will be stored securely, how long it will be stored for and how it will be used (i.e. that the recording will not be used for any other purpose except for direct care without the patient's express permission). If a recording is made this must be stored securely in the patient's clinical record. Follow your organisational policy on secure management of patient data. If recording, confirm when the recording starts and stops.

Document in the patient's record that the consultation is via video*, the nature and extent of the examination has been explained to the patient in advance (together with all the other aspects of the consultation) and the patient verbally consented to being examined in this manner. Record discussions and decisions about capacity and consent. Ensure your clinical justification for examination and non-examination is clear.
Record who was present for the consultation, you should record their identity, including their designation and the extent of the assessment witnessed, for example 'present for the complete video-linked assessment'.

2.18 Indiscreet conversations

Remember where you are when you are having confidential conversations especially when using mobile telephones. It is not appropriate to discuss personal information in hallways, corridors or stairways – or any public place where you might be overheard.

Ensure that you cannot be overheard by unauthorised people when making sensitive telephone calls, or during meetings, and when you are having informal discussions with colleagues about confidential information. In these situations, if you do not need to identify patient / staff by name - then don't.

Answer phones that record messages, which are audible when played back, should be sited in areas where they cannot be overheard by anyone who doesn't need to know.

During ward rounds (or home visits) when confidential information is being discussed, staff should bear in mind that they may be overheard by others who are in the same room. Whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the individual's rights.
Real identifiable data should not be used in training, testing systems, or demonstrations without explicit consent.

2.19 Safe havens

Although "safe havens" originally referred to the siting of fax machines, the meaning has since been expanded to encompass all secure points at which confidential information is received. As well as identifying the routine flows of person identifiable information to and from the organisation. Trust services should ensure that there are procedures in place to ensure the information is **received** to a secure and protected point. All points of receipt should be considered i.e. transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information etc.

In non-clinical areas, each site or department should have at least one designated safe haven contact point. Ideally, all information transmitted to the Trust should pass to these contact points. Clinical environments should operate in accordance with safe haven principles and the **Trust should operate safe haven procedures for all flows of person identifiable information.**

Secure receiving points
Whatever method is used, safe haven procedures should stipulate that the addressee or recipient acknowledge receipt of the information. Additionally, all staff members must be made aware of their own responsibility for ensuring the protection of person identifiable information received into a safe haven.

If the internal mail system is being used to receive person identifiable or sensitive information, it is essential that physical security measures, such as key coded or swipe card entry, are in place to protect information in the post-room, post collection point or similar.

Emails containing person identifiable or sensitive information must be stored appropriately on receipt, e.g. incorporated within the health record, and deleted from the email system when no longer needed.

A fax machine used to receive person identifiable or sensitive information must be located in a secure environment. Additionally, the faxes should be removed from the machine on receipt. The sender should be contacted to confirm receipt and the fax appropriately dealt with and safely stored.

Note: The Trust strongly discourages the use of faxes. Please use secure emails rather than faxes where possible.

Recorded telephone messages containing person identifiable or sensitive information, e.g. the names and addresses of applicants phoning for a job, or patient details, must be received into a secured, password protected voicemail box, so that only those entitled to listen to the message may do so. The department responsible for telecommunications should ensure that a password is required to gain access to messages.
A deputy should be appointed for times of absence, a group password issued or an administrator password made available. Any messages for absent staff members should also be stored securely.

2.20 Legal implications

The laws of the land have to be upheld:

- Common Law Duty of Confidentiality;
- General Data Protection Rule 2016 (GDPR) & Data Protection Act 2018
- Access to Health Records Act 1990;
- Crime and Disorder Act 1998;
- Human Rights Act 1998;
- Public Interest Disclosure Act 1998;
- Health and Social Care Act 2001;
- Freedom of Information Act 2000;
- Computer Misuse Act 2000;
- Children Act 1989;
- Equality Act 2010;
- Race Relations (amendments) Act 2000.

Data Protection Legislation is designed to control the use, storage and processing of personal data in any format - especially where there is a risk to personal privacy.

What do you do if in doubt about handling personal identifiable information?
If you are in doubt as to whether you should share the information with one of your colleagues, seek the advice of your manager, Caldicott Guardian, Information Governance lead/Caldicott Support Function or Care Group Caldicott Champion,.

Breaches of this policy could be regarded as Gross Misconduct and may result in serious disciplinary action up to and including dismissal. Careless or deliberate misuse of personal identifiable information may result in prosecution for that organisation, and in some cases, of the individual concerned.

Common law duty
All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty to support professional ethical standards of confidentiality. Everyone working for or with the NHS who records, handles, stores or otherwise comes across information that is capable of identifying an individual patient, has a personal common law duty of confidence to patients and to his or her employer.

This also includes students, voluntary staff and trainees on placements. It is recommended that such staff sign a confidentiality agreement.

Remember you are bound by the same rules of confidentiality whilst away from your work-place as you are when you are at your desk.

2.21 Implied consent

The Common Law requires that consent must normally be sought before disclosing or using personal information that is held in confidence. It is generally accepted that this consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the use or disclosure should not reasonably surprise the person concerned. Under GDPR, NHS organisations do not rely on consent for holding information. The lawful basis for holding and processing information under GDPR is Article 9 (2) h. In other circumstances and for other purposes consent cannot be implied and so must be specifically sought. The Care Record Guarantee (NHS and / or Social Care) sets out what service users have a right to expect. See quick reference flow charts at the beginning of this policy for disclosure models and examples of when consent is needed.

There are exceptions where the organisation believes that the reasons for disclosure are so important (sometimes termed a public interest justification or defence) that they override the obligation of confidentiality (e.g. to prevent someone from being seriously harmed).

Disclosure may also be required by court order or under an Act of Parliament, i.e. there is a statutory basis for the disclosure. Of particular note in this respect are disclosures permitted under section 251 of the NHS Act 2006, formerly known as section 60 of the Health and Social Care Act 2001. Applications for approval to use Section 251 powers are considered by the Confidentiality Advisory Group (CAG) of the Health Research Authority.

The advice of specialist staff, e.g. Caldicott Guardians or legal advisors should be sought prior to making disclosures in the public interest or where a statutory basis is provided as justification.

Individuals retain the right to restrict the disclosure of information even where it might directly impact on the care that can be provided.

In general no-one may consent on behalf of another individual who has the capacity and competence to decide for themselves. However, treating clinicians, parents of young children, legal guardians, or people with powers under mental health law, e.g. the Mental Capacity Act 2005 may make decisions that they believe are in the best interests of the person concerned.

It should also be borne in mind that an individual has the right to change their mind about a disclosure decision at any time before the disclosure is made, and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of personal information.

2.22 Lack of capacity to consent to disclosure of information

As the Law stands, nobody is able to give consent on behalf of another adult. If a patient is unconscious or unable to give informed consent or make a decision due to his / her physical or mental condition, then the decision to pass on information is usually taken by the healthcare professional concerned. This decision should also take into account the best interests of the patient and views of relatives and carers.

2.23 Passing on information for children and young people

Young people aged 16 or 17 are regarded as adults for consent to treatment and are entitled to the same duty of confidence as adults. Children under 16 who have the understanding to make decisions about their treatment are also entitled to decide whether personal information may be passed on. In other instances, decisions to pass on personal information may be taken by the person with parental responsibility, in consultation with the healthcare professionals involved.

In child protection cases, the overriding principle is to ensure the best interests of the child. Therefore in the case of a healthcare professional having knowledge of abuse or neglect, this information may be shared with other professionals in a strictly controlled manner, so that decisions relating to the welfare of the child can be made (see Access to Health Records Policy)

-).

2.24 Victoria Climbie□□ Guidance Note

In April 2001 Lord Laming was asked by government to chair an independent inquiry (VICTORIA CLIMBIÉ HMSO 2003) into the death of Victoria Climbie□. General recommendation 12 of□ the inquiry recommended that 'front line staff who regularly come into contact with families with children must ensure that in each new contact, basic information about the child is recorded. This must include the child's name, address, age, primary carer, GP and the name of the child's school if of school age. Also gaps in information should be passed on to the relevant authority in accordance with local arrangements.' The essence of this requirement is that being in possession of even very basic information about children can ultimately safeguard them from harm. The following details should be updated regularly. Information should be recorded under a safeguarding title in clinical records.

Recording of address - this will be that which is seen as the child's permanent address not an address that they may stay at on a temporary basis, for example 'where they may stay at the weekend with an absent parent or other family member'.

GP - although we would record the lack of GP, DOH guidance tells us we cannot notify the authority of this though we should recommend strongly that any child should be registered.
Name of primary carer/s – usually this would be the person/s with parental responsibility, normally the mother or father.

A primary carer may also be an extended member of the family such as grandparents, uncles, aunts or others who by formal or informal arrangements are the main carers of the child/ren such as foster parents or family friends. Also note, for any child born from 1st December 2003 a father now acquires parental responsibility either by being named on the certificate at the time of registration or at a later date through re-registration.

Should a patient or client refuse to share information about their child/ren, this should alert any worker to a potential child care concern. If no concern is evident then refusal to share information should be noted where the information would normally be recorded.
In the case of refusal to share information and child protection issues are evident or suspected within the family, then other sources of information gathering / sharing should be considered, such as, Social Services, Health visitors or other professionals.

If anyone is unsure how to inform the relevant agency about gaps in any of the recorded information, the safeguarding department Tel 01244 385025 may be notified who will then inform that agency involved on your behalf.

The advice of the safeguarding department Tel 01244 385025 should also be taken if a worker is concerned that a refusal to share information is linked to other concerns about a child/ren. Also see Safeguarding children policy

2.25 Statutory restrictions for passing on information

Staff must not allow personal details of individuals to be passed on or sold for fund-raising or commercial marketing purposes. There are also statutory restrictions on the disclosure of information relating to HIV and AIDS, other sexually transmitted diseases, assisted conception and abortion see below.

1. The NHS (Venereal Diseases) Regulations 1974 and the NHS Trusts (Venereal Diseases) Regulations 1991 prevent the disclosure of any identifying information about a patient with a sexually transmitted disease (including HIV and AIDS) other than to a medical practitioner in connection with and for the treatment of the patient, or to prevent the spread of the disease.

2. The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology Act 1992, limits the circumstances in which information may be disclosed by centres licensed under the Act.

3. The Abortion Regulations 1991, made under the Abortion Act 1967, limit and define the circumstances in which information submitted under the Act to the Chief Medical Officer may be disclosed.

2.26 Information sharing policy

- A high level of general principles for sharing information between the Trust and outside agencies e.g. Social Services has been agreed. Where Community Mental Health Teams are co-located, the teams have one combined record (health record contains Social Services records). Health are the holder of the record for the purposes of Data Protection Legislation. Staff guidance regarding sharing of information and answering service user queries may be found in the Information Sharing Policy

2.27 Information sharing with carers

There should be effective communication with carers.
Good practice checklist (taken from carers and confidentiality in mental health – information sharing issues. For full document see Carers and confidentiality in mental health

Carers are given general factual information, both verbal and written about:

- The mental health diagnosis;
- What behaviour is likely to occur and how to manage it;
- Medication – benefits and possible side-effects;
- Local in-patient and community services;
- The Care Programme Approach (CPA);
- Local and national support groups.

Carers are helped to understand:

- The present situation;
- Any confidentiality restrictions requested by the patient;
- The patient's treatment plan and its aims;
- Any written care plan, crisis plan or recovery programme;
- The role of each professional involved in the patient's care;
- How to access help, including out-of-hours services.

2.28 Breaches of Confidentiality/Lost Records

If there is a breach of confidentiality or lost / stolen records an incident form must be completed. Any incidents relating to Data Protection / confidentiality issues must be notified to the Trust Records & Information Governance Manager. The aforementioned manager will liaise with the Caldicott Guardian. Unless there are overriding risk issues the data subject will be informed verbally and then by letter, this includes instances where family members are members of staff and confidentiality has been accidentally breached. If confidentiality has been breached by transferring information electronically e.g. email, staff must ensure that the information is deleted from their system and then

removed from their deleted items file. Records should be retained of telephone calls relating to breaches of confidentiality to external stakeholders. The Information Governance & Data Protection Sub-Committee will review breaches of confidentiality as a standing agenda item.

2.29 Use of electronic systems

Staff who access electronic systems, e.g. SYSTMONE, EMIS, IAPTUS, PCMIS etc., should do so on a strictly `need to know basis' e.g. for clinical care of the patient. Managers can request that access to a record is audited and will be sent an audit trail of staff accessing the system to ascertain whether there is any inappropriate access. In the event of inappropriate access, staff will be subject to disciplinary action. The Information Governance & Data Protection Sub-Committee will review incidents of inappropriate access to electronic systems as a standing agenda item.

2.30 Press and broadcasting

The Head of Communications must be contacted in the event of a media enquiry (see Media Relations Policy). Before any personal information can be passed on to the media, consent must be obtained. If a person is unable to make a decision, providing basic information may sometimes be justified e.g. by correcting misleading or damaging speculation. Where possible relatives should be consulted, taking into consideration their feelings and possible distress. If someone who uses or who has used Trust services has invited the media to report his or her treatment, then the Trust may make comment but should confine itself to factual information.

If in doubt, legal advice should be sought from the Trust's Solicitors. The Trust Complaints Manager should be informed before contacting the Trust Solicitors.

2.31 Passing on information in connection with serious crime

Passing on information to help prevent, detect or prosecute serious crime may sometimes be justified to protect the public. Although there is no absolute definition of serious crime, section 116 of the Police and Criminal Evidence Act 1984 identifies some serious arrestable offences, which include:

- Treason;
- Murder;
- Manslaughter;
- Rape;
- Kidnapping;
- Certain sexual offences;
- Causing an explosion;
- Certain firearm offences;
- Taking of hostages;
- Hijacking;
- Causing death by reckless driving;
- Offences under the prevention of terrorism legislation.

Also, making a threat which if carried out would be likely to lead to:

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

In other cases Heads of Service may need to seek legal advice before taking a decision to release information. The Complaints Manager should be informed before contacting the Trust Solicitors.

2.32 Supplying of information to the police

As the Trust provides a range of services from various locations within the police force areas, when Police Officers seek clinical information or statements, Trust staff must follow the procedure as agreed by the Trust. For incidents relating to safety i.e. missing patients, suspected criminal activity, reporting of harm, loss or damage CWP staff must only disclose information necessary to assist the Police to ensure their processes are effective, in the best interest of all and in accordance with CWP policy.

Procedure

All police requests for information or statements from Trust staff should be made to the appropriate manager of that member of staff, and that manager will then act as the liaison with the Police. For safeguarding inquiries, see the separate policies respectively.

A request in the first instance should be made by telephone to the manager, giving brief details of the nature of the enquiry. The request should then be confirmed in writing giving sufficient details to enable the Trust to act upon it, by a Police Officer not below the rank of Inspector (see appendix 1 for model pro forma).

Written consent from the data subject, where appropriate, should also accompany the request (see appendix 2).

When practicable, at least 24 hours notice should be given to enable the necessary information to be gathered.

On receipt of the request, the manager will contact the Clinical Director to discuss it. As confidentiality plays a major part in these matters, care must be exercised in handling the request. If in doubt, advice from the Trust's solicitors should be sought. The Complaints Manager should be informed before contacting the Trust Solicitors.

If after discussion permission to interview staff is refused, the manager will inform the Police Inspector of this.

The manager can refuse the Police request if he / she does not believe it to be legitimate, but the Police have a right of appeal to the Chief Executive of the Trust and to the Court.

Where permission is given by the Clinical Director and manager for the member of staff to provide clinical information or statements, then the following applies:

- The manager will arrange for the member of staff to be interviewed by the appropriate Police Officer;
- A manager and / or the Trust's solicitors should be present during the interview. This is because many staff will be inexperienced in matters of confidentiality and disclosure of information, and may therefore be hesitant in their replies to Police questioning. It is for these reasons that they should be accompanied;
- The member of staff can refuse to give the Police a statement, but may later be summonsed to Court and treated as a hostile witness;
- The member of staff can choose to write the statement themselves, or elect to have the statement written on their behalf by the Police Officer. If appropriate, the health records can be used for reference purposes;
- If the Trust's solicitors are not present when the statement is made, the statement can be checked by them if required, before submitting to the Police Officer. Amendments may be necessary on the advice of the Trust's solicitors;
- The member of staff who provides the statement may be asked to attend a Court hearing, and whenever possible their availability will be checked before listing for a date;
- A brief written summary of the response given to the Police should be kept. A copy of any written statement given should also be requested and kept.

Enabling informing sharing in the public interest
The following legislation enables information to be shared without seeking consent e.g. if you believe someone has committed a crime, the Crime and Disorder provisions in section 115 of that Act state you can share this sort of information with, say, the Police. However, this type of legislation does not enforce you to do so. Decisions to share should be made on a case by case basis, in the public interest.

1. Child Protection (Children's Act 1989 and The Protection of Children Act 1999). Allows information to be shared if a child is considered at risk, e.g. Child Protection.
2. Prevention and Detection of Crime (Section 115 of the Crime and Disorder Act 1998) - e.g. requests from the Police where someone is suspected of committing a serious crime.
3. Disclosures to a health professional within a Sure Start team under the NHS Act 1997 where disclosures directly and only support healthcare of young children. (If health records are to be held within partner organisations, parents must be properly informed).
4. Data Protection Legislation provides that the non-disclosure rules will not apply if information sharing is required for:
    - The prevention or detection of crime
    - The apprehension or prosecution of offenders
    - The collection or assessment of any tax or duty

The police may request information under the Data Protection Act 2018. The Act provides that disclosures required by law or made in connection with legal proceedings are also exempted from non-disclosure. However, the decision to disclose must be weighed against the individual's rights of data protection.

3. Duties and responsibilities

3.1 Chief Executive
The Chief Executive has overall responsibility for confidentiality in the Trust. As the accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Confidentiality is the key to this as it will ensure that personal information is appropriately safeguarded at all times.

The Trust has a particular responsibility for ensuring that it responsibilities for the adoption of internal and external governance requirements.

3.2 Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The CWP Caldicott Guardian is the Medical Director, Effectiveness and Medical Workforce.

3.3 Senior Information Risk Owner (SIRO)
The SIRO (Senior Information Risk Owner) has responsibility for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO should:

- Lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its customers;
- Own the organisation's overall information risk policy and risk assessment processes and ensure they are implemented consistently;
- Advise on the management of information risk and provide assurance;
- Own the organisation's information incident management framework.

The CWP SIRO is the Director of Finance.

3.4 Information Governance & Data Protection Sub-Committee

The Information Governance & Data Protection Sub-Committee (IG&DPSC) is responsible for ensuring that this policy is implemented, through the Information Governance work plan, and that the confidentiality system and processes are developed, co-ordinated and monitored. The IG&DPSC monitors breaches of confidentiality as a standing agenda item.

Any new or proposed changes to processes will be identified and flagged with the IG&DPSC. The IG&DPSC should be consulted during the design phase so that they can decide whether a full data protection impact assessment is required for a particular project.

Where the proposed new process or system is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate privacy impact assessment should be carried out.

All staff members who may be responsible for introducing changes to processes must be effectively informed about the requirement to seek approval from the group that considers confidentiality and data protection compliance issues.

3.5 Information Governance Lead/ Caldicott Support Function/Data Protection Officer

The Information Governance Lead/DPO is responsible for the overall development and maintenance of confidentiality practices throughout the Trust, in particular for drawing up guidance for good confidentiality practice and promoting compliance with this policy in such a way as to ensure that personal information is appropriately safeguarded at all times. The Information Governance Lead/DPO supports the Caldicott Guardian.

3.6 Local managers/Caldicott Champions

The responsibility for local confidentiality is devolved to the relevant directors and managers. Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of confidentiality within their units. Care Group and Corporate Caldicott Champions provide general support to the Caldicott Guardian in relation to confidentiality issues and promoting good Caldicott practice within care groups and corporate services.

3.7 PALS officer

The Patient Advice and Liaison Service (PALS) is an accessible, confidential, free service that supports service users, carers, relatives and friends by listening to their views and concerns. It aims to resolve problems and concerns quickly before they become serious, negotiating solutions to concerns before they become complaints. PALS staff liaises with and complements the work already being done by clinical staff such as doctors and nurses. It is an information point for service users, carers and families and will sign post enquiries regarding confidentiality issues to the most appropriate member of staff.

3.8 All staff

All Trust staff, whether clinical or administrative, have a duty to keep all information confidential. They have a contractual obligation to ensure confidential and Person Identifiable Data is secure all at times. The framework for this obligation is defined in:

- The Code of Conduct for Employees in Respect of Confidentiality;
- The NHS Code of Practice on Confidentiality 2003;
- The General Data Protection Legislation 2016 & the Data Protection Act 2018;
- The Caldicott Guardian principles;
- Trust Information Governance Policies.

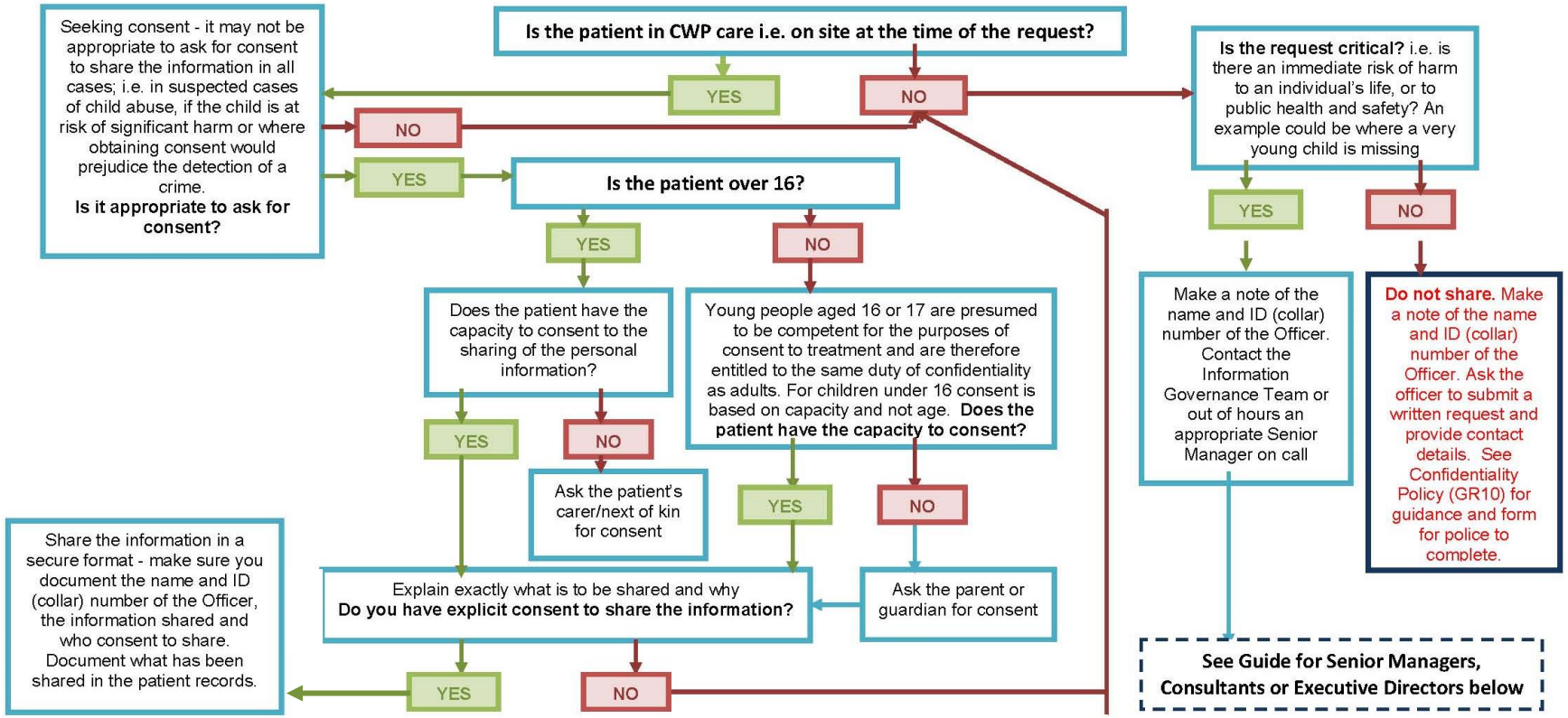
Staff must not access records without authority, discuss personal details in inappropriate venues, and transfer personal information electronically without encrypting it (see ICT Policy). All staff have a confidentiality clause within their Trust contracts of employment. All staff must complete mandatory Information Governance training. There will be disciplinary sanctions for failure to comply with duties which may result in dismissal or bringing criminal charges.

Appendix 1 - Requests for patient information by the Police

Patients have the right to expect that information gained in the course of their treatment and care is given to no-one except those involved in their care. Despite this, there are instances when disclosure to the Police will be appropriate without necessarily having the patient's consent.

Staff must not share any personal information with the Police without appropriate explicit consent (this can be verbal, but should be documented) or an appropriate legal basis (the decision to what constitutes an appropriate basis should only be made by certain staff as per the flow chart below). If in doubt always seek advice.

When the police make a request for personal information this flowchart should be used to assist staff in deciding what steps to take. This is a guide only and must be used in conjunction with the law and Trust policy. Requests should be handled by an appropriate senior staff member wherever possible.



Remember to document information sharing decisions:

- If it is decided that information should not be shared, document this in the patient record **clearly stating** the reason for non-disclosure.
- If it is decided that information should be shared, place any documentation from the police in the patient records and make a record of what information has been shared **clearly stating** the reason for making the decision to share the information.

Further advice, guidance or training please contact:

Information Governance Lead/DPO – Tel: 01244 397384
Email: gill.monteith@nhs.net

Poster Version 3: February 2014 adapted for CWP
Original version produced in conjunction with Cheshire Constabulary

Guide for Senior Managers, Consultants or Executive Directors

When making a decision to share, it is important to remember that a duty of confidentiality is owed to our patients; information cannot be disclosed, except in the following cases:

1. Disclosure required by law. For example;
   - Data Protection Legislation permits disclosure in the specific circumstances in relation to the prevention or detection of crime. Factors that may be considered when deciding this include: whether there is a threat to public health and safety, whether there is a risk of death or serious harm to the patient or other individuals and the circumstances of the matter under investigation. A police disclosure form should usually be completed (see next page forsample form).
   - Section 172(2) Road Traffic Act 1988
   - Or The Trust has been supplied with an appropriate court order
2. Have we sought / do we have the consent of the patient? Even when the patient is not present it may be necessary to seek the consent of the individual concerned before sharing any information.
3. Another overriding public interest i.e. disclosure is in the vital interests of the data subject (GDPR Article 23).

CHESHIRE CONSTABULARY

Request for Disclosure of Personal Information
Under Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d)

To:

**Check mark as is appropriate*

1. **I am making enquiries which are concerned with:** *(Note 1)*

   ☒ The prevention or detection of crime*

   ☒ The apprehension or prosecution of offenders*

   ☐ Protecting the vital interests of a person*

   ☒ I confirm that the personal data requested below is needed for the purposes indicated above and a failure to provide that information will be likely to prejudice those matters.

   ☐ I confirm that the individual(s) whose personal data is sought should not be informed of this request as to do so would be likely to prejudice the matters described above.

2. **Information Required:** *(Note 2)*
   Name of patient
   Dates of records required
   Purpose of records required

3. **Police Reference:** *(Note 3)*
   Police investigation number and details of investigation

Where details are not supplied this form must be counter signed by a Senior Officer (Inspector or above)

4. **From:**

   Rank/Number/Name:

   Station:

   Date/Time:

   Telephone Number(s):

   Email address:

I am aware of the provisions of the Data Protection Act 2018 regarding the offences relating to the unlawful obtaining etc of personal data.

Signature:

(Note 4)

Counter Signature:

Rank/Number/Name: Click or tap here to enter details of person providing counter signature.

Please see Guidance Notes on following page

Guidance Notes

This form replaces the Section 29(3) form, which has become redundant by virtue of new data protection legislation. It is used by the police as a means of making a formal request to other organisations for personal data where disclosure is necessary for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. It places no compulsion on the recipient to disclose the information, but should provide necessary reassurance that a disclosure for these purposes is appropriate and in compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

NOTE 1 DPA 2018 Schedule 2 Part 1 Paragraph 2 provides an exemption for organisations to disclose personal data to the police where disclosure is necessary to support any of the crime purposes. The exemption means that an organisation can provide personal data without fear of breaching the GDPR or DPA.

For the avoidance of doubt, Cheshire Constabulary is Competent Authority as specified in Schedule 7 of the DPA and processes personal data which is necessary for the performance of a task, carried out for the law enforcement purposes as defined in Part 3, DPA.

Request for information pertaining to protection of life
GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure *is necessary in order to protect the vital interests (life or death situation) of the data subject or of another natural person.*

NOTE 2 Give sufficient information for the organisation to identify an individual on their records. You should include the name of the individual and any other information you feel is relevant. For example, when requesting information from a bank, supply the account number, if known.

Also, state what information you require to support your enquiry. You should not ask for 'all information known about individual' or similar. You must ask for specific information.

NOTE 3 Give enough information in order to allow the organisation to make a decision regarding disclosure. However, do not supply excessive information, which is not required to resolve your enquiry. If the enquiry is particularly sensitive, and you do not want to supply further details, the form must be signed by an officer of Inspector rank or above.

NOTE 4 The Investigating officer should be aware that they are making a statement to the effect that obtaining personal data under false pretences may constitute a criminal offence.

Further guidance on the use of this form may be obtained from the force Data Protection Officer.

A COPY OF THE COMPLETED FORM MUST BE ATTACHED TO THE RELEVANT OCCURRENCE FOR AUDIT TRAIL PURPOSES

Appendix 2 - Consent to share health records with police

To whom it may concern

I (print name) _____

DOB _____/_____/_____

Address _____

give consent for Police to access certain relevant areas of my health records held at _____ as agreed with me beforehand for the purpose of gaining relevant information to the case currently being investigated by them.

Signed by _____

Date _____/_____/_____

Appendix 3 - Simple patient consent to share reports

I am happy for a copy of the report written about me by:

Name	
Position	
To be shared with	
Name	

Signature		Date	

The purpose of _____ reading the documents and who might see it, was explained to _____ by:

Name		**Position**	
Signature		**Date**	

Name		**Position**	
Signature		**Date**	

This form will be kept in a file

The words will be put on a computer

Appendix 4 - Consent to pass on contact details to other families (sample)

I _____ parent / carer of _____ agree to LD

CAMHS passing on my contact details to other families, to enable them to contact me, for the purpose

of _____.

I also understand that LD CAMHS are not responsible for the actions of third parties following the exchange of contact details.

Name (printed)			
Signed (Parent / Carer)		**Date**	

Name (printed)			
Signed (Community Nurse)		**Date**	