Leeds and York Partnership
NHS Foundation Trust

Confidentiality Code of Conduct

The key messages the reader should note about this document are:

1. Understand what it means for information to be “Confidential”.
2. That appropriate sharing of information can be as important as confidentiality.
3. Tells you who to contact for advice and support on confidentiality issues.
4. That everyone working for or on behalf of LYPFT has a duty to keep confidential information confidential.
5. That this is a legal requirement, and there can be consequences in law for both the Trust and for the reader when we fail to maintain confidentiality.
6. Sets out the expectations of confidentiality for agile working.

This policy/procedure may refer to staff as qualified/registered/professional or other such term to describe their role. These terms have traditionally referred to individuals in a clinical role at band 5 or above. Please note that the use of these terms **may or may not** include nursing associates or associate practitioners (band 4). For clarification on whether a nursing associate or associate practitioner is an appropriate person to take on the identified roles or tasks in this policy/procedure please refer to the job description and job plan for the individual, or local risk assessment.

DOCUMENT SUMMARY SHEET

ALL sections of this form must be completed.

Document title	Confidentiality Code of Conduct
Document Reference Number	IG-0003
Key searchable words	Confidentiality, IG, Data Protection, Caldicott
Executive Team member responsible (title)	Chief Financial Officer
Document author (name and title)	Carl Starbuck – Head of Information Governance
Approved by (Committee/Group)	Information Governance Group
Date approved	28 October 2022
Ratified by	Policy & Procedure Group
Date ratified	10 November 2022
Review date	10 November 2025
Frequency of review	*At least every three years*

Amendment detail

Version	Amendment	Reason
0.1	Transposed into new procedural document format	
0.2	Review amendments made by Carl Starbuck and Claire Stoker.	Development work in line with current IG best practice.
0.3	Review amendments made by Carl Starbuck and Claire Stoker.	Following input from IG Steering Group delegates
0.4	Minor changes by Carl Starbuck	Following IG adoption of policy from HR's lead. Re-align document ownership and approval / ratification committees
1.0	Ratified by IM&T Committee	
1.1	First review by Carl Starbuck	Approaching review date. Appendix C, disclosures to police added.
2.0	Ratified by ET	Ratified by Executive Team 31st January 2012
2.1	Second review by Carl Starbuck	Review date reached. Transposed into current document template, large scale review of all content, modernisation of committee structures, language and terminology.
3.0	Ratified	Policy & Procedure Group
3.1	Review and refresh	Alignment to the EU General Data Protection Regulation – April 2018
4.0	Ratified	Policy & Procedure Group ratification – 29 August 2018
5.0	Changes to reflect "Care Services" and "Head of Operations" structure and naming conventions	Review undertaken aligned to instructions received from Peter Johnstone (24/12/2019) Actions completed 07/01/2020
5.1	Regular review due August 2021. For review by IG Group 22nd August 2021	Reviewed as required, for approval by IG Group. Key changes:- Reflect BREXIT-related GDPR / DPA issues Update key contacts Reflect NHS trajectory re. fax machines Modernise digital media references Strengthen agile working section Update Caldicott Principles (Dec. 2020)

6.0	Ratified	Policy & Procedure Group ratification – 12th August 2021
7.0	Appendix E & F added	Additions made at the recommendation of the Auditors when reviewing evidence for the 2021-2022 DSP Toolkit – establishing a need to present national policy for Registration Authority (SmartCards) & the National Data Opt-Out in a local policy document.

CONTENTS

1. Confidentiality Code of Conduct

1.1 Flow Chart <Not Applicable>

1.2 Executive Summary

All employees working in the NHS are bound by the common law duty of confidence to protect Personal Confidential Data, and commercially sensitive information they may come into contact with during the course of their work. This is re-enforced by the requirements of the Data Protection Act (2018) – the UK enactment of the General Data Protection Regulation (UK-GDPR), the Human Rights Act and other relevant legislation, and for health and other professionals through their own professional codes of conduct and contracts of employment.

The Code gives a detailed definition of confidential information and the approach to dealing with requests for information from a variety of sources.

The Code also covers internal and external movement of information and its storage and eventual disposal when no longer required. Additionally there is instruction on agile working, as working outside the Trust's normal places of business raises additional threats to confidentiality that we must be aware of.

If any employee requires an explanation concerning the interpretation or the relevance of this Code, they should discuss the matter with their line manager, the Information Governance Team or the Caldicott Guardian.

The Code is over-arched by the Trust Information Governance Policy and is a key procedural document in the Trust's overall approach to Information Governance and the Information Governance Framework. The Code is supplemented by other Trust Information Governance procedural documents and guidance, which are signposted throughout.

1.3 Confidentiality – What is it?

Confidentiality is perhaps best described as the rules and behaviours that must be in place when 2 or more people (or organisations) share information, with a mutual understanding that the information will not be shared further unless those rules are satisfied, or the person who shared the information is happy for it to be shared. Information shared between a service user and a healthcare professional or service is held under a duty of confidence.

1.4 What do we Regard as Confidential Information?

As a general rule, we regard all service user information as confidential.

The Data Protection Act (2018) classifies both "Personal" and "Special Category" information as follows:

- Personal = only includes information relating to natural persons who:
    - can be identified or who are identifiable, directly from the information in question; or
    - who can be indirectly identified from that information in combination with other information.

- Special Category = information which is
    - personal data revealing racial or ethnic origin;
    - personal data revealing political opinions;
    - personal data revealing religious or philosophical beliefs;
    - personal data revealing trade union membership;
    - genetic data;
    - biometric data (where used for identification purposes);
    - data concerning health;
    - data concerning a person's sex life; and
    - data concerning a person's sexual orientation.

The Data Protection Act (2018) gives extra protection to *"personal data relating to criminal convictions and offences or related security measures"*. We refer to this as criminal offence data.

This covers a wide range of information about:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

It includes not just data which is obviously about a specific criminal conviction or trial, but also any other personal data relating to criminal convictions and offences, including:

- unproven allegations;
- information relating to the absence of convictions; and
- personal data of victims and witnesses of crime.

It also covers a wide range of related security measures, including

- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty if not adhered to.

It can be seen from these definitions that information which is patient-identifiable is Special Category, because to identify a service user is to identify them as a user of healthcare services, which meets the definition of Special Category data.

It is notable that as well as health conditions – and thus medical records – being regarded as sensitive under the Act, our records frequently contain other strands of the Special Category data definition. Ethnicity and sexuality are often recorded in our service user's records, as is forensic data.

Whilst we do not ordinarily see the identities of staff carrying out their professional role as being confidential – as we are paid by the public purse and thus accountable for our actions and necessarily visible in these roles, we regard the private lives, home addresses, and any Special Category data relating to our staff as similarly confidential.

It should be noted that although the Data Protection Act (2018) is our primary legislative framework for considering the confidentiality of information in our possession, the common law duty of confidence which is implicit in information shared between service users and our staff continues post-mortem. As the Data Protection Act (2018) only covers information relating to the living, the Caldicott 2 Review 2013 – *Information: To Share or Not To Share* – gave healthcare a new terminology to capture confidential data for both the living and the deceased:

Personal Confidential Data (PCD) shall be used going forward throughout this document.

As a final definition of what we regard as confidential, aside of Data Protection definitions, we regard some corporate business information as confidential (where it is not subject to disclosure under the Freedom of Information Act), and personal staff information (banking details, personal addresses and telephone numbers, next of kin & emergency contacts, NI numbers etc.) as being confidential.

1.5 Our Obligations

The NHS Care Record Guarantee, distributed to households across the UK, made promises to the people we serve regarding how we will use healthcare records. We will observe and respect these promises. See Appendix A for links to the NHS Care Record Guarantee.

The Data Protection Act (2018) sets out key principles governing the use of personal information. We will observe and respect these principles. See Appendix B for the Data Protection Principles.

The Caldicott Principles, last updated in December 2020, set out 8 principles guiding the use of service user, staff, and other personal information in health and social care. We will observe and respect these principles. See Appendix C for the Caldicott Principles.

Above all we will respect the confidentiality of the people we serve and the information we hold, and will maintain those confidences unless the law requires otherwise.

1.6 Gathering & Recording Information

The Data Protection Act (2018) Principles state that personal information must be:-

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

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

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

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK-GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

From these principles we understand that we must only gather information which is relevant to the services we are providing, only record information which is relevant for this purpose and not gather and record information which would be seen to be excessive for this purpose. There is also an obligation in law to maintain accurate records.

The fair & lawful processing requirement tells us that we must only gather, record and use personal information in a way which complies with the law, and which is deemed fair because it meets the reasonable expectations of the data subjects – i.e. the person the information is about. We achieve this by informing data subjects how we will use their information by issuing a "Privacy Notice" – so that our use of people's information is transparent.

1.7 Using and Accessing Information

Having defined that we must use information fairly and lawful, it follows that fair and lawful processing will only be met when information is used appropriately. We ensure this is the case by only accessing information with which we have a "legitimate relationship".

A legitimate relationship exists when, for example, a service user is referred to a care team. The members of the team are providing that service user with care – and it is therefore justifiable to access the service user's information to provide that care in a safe & effective manner.

It is inappropriate and unlawful to wilfully access personal information where no legitimate relationship exists. To do so is a criminal offence; and if computerised data is accessed wilfully inappropriately, a criminal offence is committed under the Computer Misuse Act (1990).

1.8 Medical / Non-Medical Purposes

The Data Protection Act (2018) Principles tell us that information must only be used for one or more defined purposes. Our Privacy Notices will tell data subjects – the person the information is about – how we will use their information, and for what purpose. Information must only be used for the purpose(s) for which it was originally obtained, unless the law requires or allows it to be used for another purpose, or the data subject gives their consent for the information to be used for this other purpose.

As an example, we collect service user information for the purpose of providing them with healthcare services. This principle allows the information to be used by healthcare professionals for this purpose. As an extension of the principle, service user information can be used for the management and quality assurance of healthcare services. We see this as the primary purpose of the information, with anything else deemed a secondary use.

The law allows information to be used for other purposes without consent. These include sharing information with the police for the detection and prevention of crime, used to support Safeguarding purposes, and for legal proceedings. These scenarios illustrate where data protection law makes the use of healthcare information lawful for non-healthcare purposes.

Whilst making use of patient-identifiable information for healthcare purposes is always permissible, authorisation should be sought from the Information Governance team and / or the Trust Caldicott Guardian for non-healthcare use of data. The Trust Caldicott Guardian is the final arbiter on all decisions relating to non-healthcare use of service user data.

1.9 Storing & Archiving Information

To maintain the confidentiality of information, its storage must be sufficiently secure. Trust systems – including our networks and applications, facilitate the secure storage of information, protected by technical measures and robust access controls. Colleagues with access to these systems must not attempt to circumvent this security,

or to weaken it by the sharing of their access credentials – usernames, passwords, smartcards, PINs etc.

Paper records must be stored using non-technical measures to protect their security. This includes ensuring that records are appropriately filed and stored – both locally at in-patient / out-patient sites, at the Trust's records storage locations, and at off-site locations.

The Information Governance Team will conduct physical security reviews at offsite archive repositories.

1.10 Records End-of-Life & Disposal

Records are retained according to the *NHS Records Management Code of Practice*, which classifies all types of service user and non-healthcare corporate records, states how long they must be kept, and the disposal arrangements at end-of-life. A copy of the Code, including its Retention Schedules, is available on Staffnet. The Information Governance Team will advise on records retention and disposal issues.

It should be noted that "disposal" does not necessarily mean "destruction". In some circumstances records may be moved to a National Archives regional centre for permanent historical archive preservation.

The Trust Health Records Policy indicates how long service user records should be retained at Trust sites, and at what point they should be moved to off-site archive.

Should any hard copy paper documents require secure disposal, these should be disposed of in confidential waste via the usual processes.

1.11 Information Sharing

A common misconception about Information Governance and Data Protection is that it is a barrier to information sharing. This is not the case. Both IG & data protection legislation are enablers of information sharing, with the Data Protection Act (2018) setting out the framework, via the enactment of UK-GDPR Articles 6 and 9, under which information can be shared lawfully for certain purposes.

The sharing of appropriate and relevant service user information with other clinicians – both within and outside the Trust – who are providing a service user with care – is permissible under Article 6-1-e and 9-2-h. This is reinforced by the 7th Caldicott Principle which was added in 2013 following the 2nd Caldicott Review, *Information: To Share or Not to Share*:-

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

They should be supported by the policies of their employers, regulators and professional bodies.

Information Sharing Agreements may be entered into to support information sharing, but it should be noted that these are neither legally required nor necessary. It is the legal framework of the Data Protection Act (2018) and other strands of law that enables information sharing, not an agreement. Without a legal basis to share information, information cannot be shared and an agreement cannot be written.

Information Sharing Agreements and Protocols do have value however. A well-written Protocol can set out the over-arching principles of an intent to share between potential sharing partners – they are typically drafted on a regional basis. An Agreement can sit under a Protocol (or stand-alone), and describes an actual, known sharing relationship between 2 or more partners for a defined purpose. As a general rule, an agreement is NOT required to share information between healthcare providers to share healthcare data for direct care purposes.

The Information Governance Team will support information sharing and assist with the development or sign-up to Information Sharing Agreements and Protocols when required.

1.12 Movement of Personal / Sensitive Information

Our work often requires that we move information – both within the Trust and to other organisations. The Data Protection Act (2018) requires us to protect the personal and Special Category data we hold.

IG-0009 – Safe Haven Guidance – gives advice on how to move information securely via internal and external mail, courier, e-mail, and on portable digital media such as USB sticks and CD/DVD disks.

It should be noted that the DHSC had previously set out to rid the NHS of the use of fax machines, given that it was outdated technology and perceived to be unsecure. Whilst at the time of writing the COVID-19 pandemic has slowed delivery of this intention, alternative methods to fax should be used – e.g. secure e-mail.

1.13 Your Conduct – Being a Personal Safe Haven

The most important aspect of information security is the “Human” element. It is not sufficient to simply consider systems and devices as the entire scope of information security, particularly with the advent of mobile / remote access and agile / hybrid working arrangements. All staff must adopt working practices so that they can be considered a “Personal Safe Haven” – essentially a safe pair of hands for personal, Special Category or otherwise confidential information.

Basic and common sense steps will help us all to meet this important obligation:-

- Maintain an awareness of your surroundings and the threats to information security in your immediate vicinity.

- Ensure information is not visible or accessible to inappropriate people.
- Beware of so-called “shoulder surfing”.
- Make sure that laptop / PC screens are not inappropriately viewed by 3rd parties, particularly when working remotely.
- Ensure PCs are locked or switched off when not in use.
- Clear desks and other workspaces of information when leaving.
- Ensure that information transferred between locations arrives intact, without total or partial loss en-route.
- Use a lockable document folio, briefcase or other secure carrier for loose papers carried between locations.
- Store information in the boot of a car when in transit.
- Take particular care to lock bicycle / motorcycle panniers.
- Remove personal, Special Category or confidential information from any vehicle on arrival at your work base, home, or final destination.
- Only take & use personal, Special Category or confidential information when working from home with the authorisation of your line manager.
- When working from home, ensure that information is used and stored securely and protected from access by family members or other visitors to your home at all times.
- Ensure that e-mail addresses are correct before sending information via any e-mail method, particularly when addresses are auto-completed by your e-mail software.
- Know and apply the Caldicott Principles to any information you are intending to send.
- Facilitate mobile / remote / agile working via secure method (NHS.net e-mail, encrypted memory stick, encrypted laptop etc). NEVER do this by e-mailing personal, sensitive or confidential information to a private / personal e-mail account or by storage on a non-Trust PC, laptop or device.
- Only use SmartPhone apps that are provided or approved by the Trust.
- Check the fax number before sending information via fax, particularly when using pre-set or speed-dial numbers.*

* It should be noted that the DHSC had previously set out to rid the NHS of the use of fax machines, given that it was outdated technology and perceived to be unsecure. Whilst at the time of writing the COVID-19 pandemic has slowed delivery of this intention, alternative methods to fax should be used – e.g. secure e-mail.

1.14 Requests for Information on Service Users

- Never routinely give out information about service users to persons who do not “need to know” in order to provide healthcare and treatment i.e. someone with direct care / responsibility for that person / information. If in doubt, seek guidance from your manager before disclosing the information.
- Service users must be advised at the outset of engaging with services that their information may be shared with 3rd parties when this is directly related to their care. Services users must also be informed of any and all secondary uses which are known at that time and permission must be sought for these uses. Informed consent must be sought from the service user for any secondary use

which has not been previously agreed. The service user has the right to refuse consent in full or in part to such sharing and their choices and decisions must be respected.

- All requests for access to person-identifiable information should be on a justified need and may also need to be agreed by the Trust's Data Protection Officer or Caldicott Guardian:-

Carl Starbuck Head of Information Governance / Data Protection Officer	**Dr Christian Hosker** Medical Director / Caldicott Guardian
tel: 07980 956666	tel: 0113 85 55914

- If you or your manager are not sufficiently sure that the information can be disclosed, seek guidance from the Data Protection Officer and / or the Caldicott Guardian.

Any decision to disclose confidential information about service users should be fully documented. The relevant facts should be recorded, with the reasons for the decision and the identity of all those involved in the decision-making. Reasons should be given by reference to the grounds on which the disclosure is to be justified. *(Mental Health Act (1983) (as amended) Code of Practice 2015, para 10.15)*

The Data Protection Act (2018) requires that we inform data subjects about uses of their information as well as being clear that we have a legal basis for the use of the information. This is what the Act calls the Right to be Informed, and it is this, along with having a legal basis, that comprises what is known as "fair and lawful processing" of personal data.

In some circumstances, we are compelled to share information with other agencies because the law requires us to do so. Sharing of this type may take place with or without consent, or in some cases without the knowledge of the service user. The reasons for this include criminal investigations, border enforcement, collection of taxes, as well as other statutory duties placed on the Trust. As these issues are often complex, disclosures for non-health purposes should always be referred to the Data Protection Officer and / or Caldicott Guardian for advice.

If you have any concerns about disclosing / sharing service user information you must discuss this with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with you should take the enquirer's details and respond to the requestor when you are satisfied the disclosure of information can take place. If your line manager feels it is appropriate, they may refer the matter to the Data Protection Officer or Caldicott Guardian.

1.15 Telephone Enquiries

If a request for information is made by telephone:-

- Always check the identity of the caller, and
- Check whether they are entitled to the information they request, and
- Take a number, verify it independently and call back if necessary.

Unless the enquiry is for direct care purposes, service user consent should be sought in these circumstances, as should their assistance in verifying the caller's identity, where possible and appropriate. Remember that even the fact that a service user is in hospital, or that a person is a service user is confidential in itself. If in doubt consult your manager.

Do not share any information unless you are confident that you are not breaching this Code, any appropriate legislation, and / or your own professional Code of Conduct.

1.16 Requests for Information by the Police and Media

With respect to the Police:-

- The Police do not necessarily have a right to instantaneously access information we hold (including records and CCTV footage).
- Requests for information from the Police should always be referred to the appropriate level of management (Head of Operations or delegated authority).

Detailed guidance on police and other disclosures to official bodies is included in Appendix D.

With respect to the Media:-

- Do not give out any information under any circumstances.
- Only the Communications Department are authorised to do so. If you receive any request from the media by personal visit, phone, e-,mail or other method, refer the contact to the Communications Team at Trust HQ.

1.17 Disclosure of Information to Other Employees of the Trust

Information on service users, staff, carers, Foundation Trust members and other individuals should only be released on a need-to-know basis.

- Always check the member of staff is who they say they are.
- This can be achieved by checking the employee's photo ID badge and / or their internal extension number or e-mail address prior to giving them any information.
- Check whether they are entitled to the information.
- Don't be bullied into giving out information.
- Communicate via an appropriately secure method.

If in doubt, check with an appropriate line manager, the Information Governance team, and / or in the case of service user information, the Caldicott Guardian.

1.18 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to themselves, their own family, friends or acquaintances unless they are directly involved in the service user's clinical care or with the employees administration on behalf of the Trust. Inappropriate action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action. This is also a breach of data protection law and could lead to the prosecution of the individual concerned and the Trust.

It is important that you disclose to your manager that you may have access to family or friends information, as soon as you become aware of it.

If you have ever been a user of our services, have access to Trust or National patient data systems, or work in certain roles (Systems Administration, Human Resources, Intranet Management, ICT etc.) you may also have access to your own records. It is strictly forbidden for you to look at your own records, although you may request a copy of your records under the Subject Access Request process.

The above point does not bar access where it is otherwise granted, e.g. online payslips, training records, Total Reward Statements etc.

Your duties within the Trust may grant you access to a variety of local and national computer-based systems. These systems must only be used for their intended purpose, and there must be a "legitimate relationship" between you, the data and the subjects of the data you are accessing. If you access systems or records inappropriately you may be prosecuted under the Computer Misuse Act (1990).

1.19 Carelessness

- Do not talk about service users in public places or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public or inappropriate staff.
- Ensure that computers are locked when not in use or left unattended.
- Take particular care when creating correspondence. Check addresses against our main records systems, ensuring that the postal address on the letter and / or envelope is correct.
- Take care when filling envelopes that only information intended for the addressee is included.
- Take particular care when collecting printing from shared printers / multi-function devices. The paperwork you pick up may include other people's printing.

1.20 Confidentiality of Usernames and Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone, except if

required by Trust IT technical staff to resolve problems. In this case, the password should be immediately reset by the user at the next log on to the relevant system.

- Usernames and passwords must not be written down.
- If you have difficulties remembering your usernames and passwords these may be stored securely in the 'Notes' function within MS-Outlook.
- Usernames and passwords must not relate to the employee or the system being accessed.
- Usernames and passwords must not be shared with colleagues.
- When usernames and passwords are initially given to staff they should be communicated securely and confidentially.

You will be given more information about password control and format etc. when you receive your training and / or password. Guidance on the creation of secure passwords is available on the ICT area of Staffnet, or by contacting the ICT Service Desk.

No employee should attempt to bypass or defeat Trust security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to your manager and may result in disciplinary action and also in a breach of the Computer Misuse Act (1990) and / or data protection legislation, which could lead to a criminal prosecution.

If you have been issued with a SmartCard and PIN code to access national information systems, you will need to store these safely and securely, and use them in accordance with the terms and conditions set out in the appropriate Registration Authority documentation. All access is monitored and checked for validity.

1.21 Agile Working – Working at Home or Other Remote Location

Agile working from home or other location as opposed to a regular 'base' has become increasingly the norm, particularly during the COVID-19 pandemic and is set to continue in the post-COVID 'new normal'. If you need to do this you first need to gain approval from your manager.

If you wish to use a Trust laptop at home to access the Trust's ICT Network or access your work emails on your home PC then please contact the ICT Service Desk for advice and also refer to the LYPFT Trust Network Access Guidelines on Staffnet. Trust-issued laptops have secure access to Trust systems via home or other broadband services.

If your manager agrees to you working at home you need to ensure the following are considered and remember that there is personal liability under data protection law and your contract of employment for breach of these requirements:

- If you work on person-identifiable information at home or remotely, this must only be with the knowledge and authorisation of your line manager.
- If you are taking paper records please ensure there is a record that you have them, where you are taking them and when they will be returned.

This is particularly important for service user records. A tracer card system or electronic tracking system should suffice. If no such system is available an appropriate manual record should be made.

- Ensure any personal information in paper form e.g. service user / staff files etc are appropriately secure prior to them being taken out of Trust building(s). Lockable briefcases, file folios or similar should be used.
- Data carried on portable digital media must be password protected and encrypted to NHS standards. Advice on how to password protect and encrypt files is available from the Information Governance team. The Trust uses hardware encrypted USB sticks for the secure transportation of confidential data to facilitate home / remote working, although this should not be necessary for staff already issued with a Trust laptop.
- Make sure records are transported in the boot of a car or carried on your person while being transported from your work place to your home or remote location.

While working at home or remotely you have a personal responsibility to ensure records are kept secure and confidential. This means that other members of your family and / or your friends / colleagues / visitors must not be able to see the content or outside folder of the records. You must not let anyone have access to the records.

If you take home computer records on portable digital media you must ensure all of the above applies. Confidential Information must not be stored on your home PC's hard drive. Trust issued USB sticks will operate as a new drive on your computer. It should therefore not be necessary to transfer data from a Trust issued USB stick to your home or other non-Trust computer.

When taking records back to work this must be carried out as above, in secure containers etc. For manual records they should be logged as being back within the Trust. For computer records on portable digital media these MUST be virus checked before being loaded onto any Trust systems – especially any which can be accessed via the network. The ICT Service Desk can advise on virus checking procedures.

Should any hard copy paper documents require secure disposal, these should be brought back to Trust premises and disposed of in confidential waste via the usual processes unless you have facilities at home which meet appropriate destruction standards – i.e. a "confetti cut" shredder which meets CPNI standards. The Head of Information Governance should be contacted to advise & approve domestic equipment on a case-by-case basis.

When LYPFT services are permanently sited in co-located or 3rd party premises, the Information Governance Team will undertake a review of data and physical security at the site prior to occupancy on request, or in response to any concerns raised.

1.22 Anonymised / Pesudonymised Information Sharing

Where disclosures of anonymised / pseudonymised information are made, e.g. reporting of incidents to the National Patient Safety Agency or other body, it is important to note that person-identifiable data may not be limited to the obvious fields. The body text of records may contain person-identifiable data, so the anonymisation process should include a review of all text provided, such that anonymisation is applied completely throughout the materials shared.

In some cases, anonymised data may be shared, whilst in others, pseudonymised data may be more appropriate.

- Anonymised = data from which ALL identifiers are removed. The data cannot be re-identified, even at source.
- Pseudonymised = data from which ALL identifiers are removed, but a single identifier is left or added which can only be re-identified from those who hold the pseudonymisation key.

The NHS number is defined as an identifier, not a pseudonym, as it can be translated and re-identified widely across health and increasingly in social care.

1.23 Key Contacts

Further details on any of the above issues are available from:

Medical Director / Caldicott Guardian	**Dr Christian Hosker**	**0113 85 55914**
Head of IG / Data Protection Officer	**Carl Starbuck**	**07980 956666**
IG Support Officer	**Anne-Marie Wilson**	**07717 941888**

2 Appendices

(or the link to the relevant document(s) on Staffnet)

Appendix A - NHS Care Record Guarantee

http://staffnet/pnp/Policies%20and%20Procedures/Document%20Library/Information%20Governance/NHS%20Care%20Record%20Guarantee.pdf

Appendix B – the Data Protection Principles

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

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

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

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK-GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Appendix C – the Caldicott Principles

1: Justify the purpose(s) for using confidential information

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

2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

4: Access to confidential information should be on a strict need-to-know basis

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

5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

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

8: 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.

Published December 2020

Appendix D – Disclosures to the Police and Data Protection Law

READ FIRST: Guiding Principles

Do not feel pressurised to give information simply because the police have requested it. It is always necessary and reasonable to ask what information is required and for what purpose before making a decision.

Whilst it would be reasonable to provide immediate assistance and information where there is a clear and present danger of serious harm (e.g. murder, rape, kidnapping, death by dangerous driving, terrorism etc.), most cases are less urgent and warrant a considered approach to disclosure.

If in doubt, seek advice from your manager.

Under data protection law, Common Law, the European Convention on Human Rights and NHS Caldicott guidance you are under a duty of confidence to keep personal / sensitive information confidential and secure.

However, data protection law also permits the use and sharing of information providing certain conditions are met. These conditions facilitate Police access to data held by the Trust, including information about service users, staff and data relating to other individuals.

Can you disclose personal / sensitive information to the Police?
The Police may approach the Trust in a variety of ways, but right of access is not always a given. The information below should assist you in deciding whether or not the Police can be given information, the scope of what they should receive, and whether or not consent of those concerned is a relevant factor.

Subject Consent.
The consent of data subjects – the person the information is about – should be sought whenever this does not compromise the investigation - e.g. by the destruction of evidence, or where there is a 'flight risk'. Subject consent is most common when a person is engaging with a Police enquiry and actively helping. Subject consent must be presented in written form.

Legal Duty Disclosures (you MUST disclose, consent is NOT required)

- **Prevention of Terrorism Act (1989) and Terrorism Act (2000)**

If you have gained information about terrorist activity you MUST inform the police.

- **Court Order**

Where the courts have made an order, you must disclose the required information, unless the organisation decides to challenge the order in court.

- **The Road Traffic Act (1988)**

You have a statutory duty to inform the Police, when asked, the name and address of any driver who is allegedly guilty of an offence under the Act; do not disclose clinical information.

Legal Power Disclosures: (you MAY disclose, but consider implications of gaining consent)

- **The Police and Criminal Evidence Act (1984)**

You can pass on information to the Police, as the Act creates a power to do so if you believe that someone may be seriously harmed. Serious arrestable offences include murder, rape, kidnapping and causing death by dangerous driving.

- **The Crime & Disorder Act (1998)**

Information may be required on an individual if there is a need for strategic cross-organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in.

- **Multi Agency Public Protection (includes the Probation Service)**

The Criminal Justice and Court Services Act 2000 sets the framework for sharing information about potentially dangerous offenders. Information about individuals may be required by 'Multi Agency Risk Conferences'. If you are requested to provide information, you should consider gaining consent / informing the individual(s) unless this may cause more harm than good. If the risk presented by an individual(s) clearly cannot be effectively managed without the sharing of information and gaining consent is inadvisable, then relevant information can be shared as it is in the interests of the public.

- **Children Act (1989)**

Under section 47 of the Children Act (1989) a Local Authority, working with other relevant agencies, must make all necessary enquiries to decide whether they should take any action to safeguard or promote a child's welfare. In such a situation, firstly confirm it is a section 47 enquiry and then release relevant information, unless 'to do so would be unreasonable in the circumstances of the case'. You do not have to gain consent of the parent or child or inform them.

If you suspect a child is being abused, but there is no request for information, you have a legal power to disclose information to Social Services (under 'vital interest' & 'healthcare purpose' conditions of the EU General Data Protection Regulation) and / or the Police (under the Police & Criminal Evidence Act). Consider whether gaining consent or informing the child and parents would be beneficial or detrimental to the situation. If detrimental then disclosure without consent is permitted.

Data Protection Act (2018)

The Police may make a written request for information when making enquires relating to:

- the prevention and detection of crime, or
- the apprehension or prosecution of offenders

and the view of the Police is that seeking consent or even informing the subject about the transfer of data will prejudice the enquiry. Providing the police with information relating to a bona-fide investigation of serious crime is permissible.

The Police will need to make a written approach, signed by a senior officer of the rank of inspector or above. Similar approaches may also be made by other regulatory agencies. The UK Borders Agency (Immigration) and Her Majesty's Revenue & Customs (Taxation) may also approach the Trust via this route.

Must we provide the Information?
No. It is for the Trust to consider the validity of disclosure and assist with this at its discretion, however the Police have usually made a considered judgement about their need for information and thus we comply with properly presented written requests.

Balancing our Police Disclosures with Service User Care
Although we seek to work co-operatively with the Police and other regulatory bodies, and we may disclose confidential information in support of Police or other enquiries, we must balance this with the care of our service users and other individuals on whom we hold information.

When we initiate preliminary discussions both internally (e.g. between service managers, Trust Police liaison contacts, and also the Trust Data Protection Officer or Caldicott Guardian), and externally with the Police etc should take place without disclosure of the identities of those concerned.

Advice can be given WITHOUT knowing the identities of those concerned.

Always direct the police to liaise with the team holding the information, so they can ensure that in identifying those concerned, the care and support needs of those who the police may contact are adequately considered.

Important notes & further advice:
Always check the identity of anyone requesting information. Only give the minimum information which satisfies the request. Seek advice from colleagues and line managers when making a decision about disclosure and record your reasoning and any decisions made. You may have to judge whether disclosing information will cause fewer problems than withholding it.

Further details on any of the above issues are available from:

Medical Director / Caldicott Guardian	**Dr Christian Hosker**	**0113 85 55914**
Head of IG / Data Protection Officer	**Carl Starbuck**	**07980 956666**
IG Support Officer	**Anne-Marie Wilson**	**07717 941888**

Appendix E – SmartCard Policy

The following represents the LYPFT SmartCard Policy, in alignment with the requirements of the NHS National Registration Authority Policy, available online via the link below.

The Trust and it's staff are required to adhere to the NHS National Registration Authority Policy at all times.

https://digital.nhs.uk/services/registration-authorities-and-smartcards#policy-and-guidance

All references to SmartCards in this document and elsewhere also encompass any use of virtualised SmartCards or alternative access tokens / credentials that achieve the same access.

It is a mandatory requirement that organisations that run local RA activity have a local policy outlining their approach. The following are mandatory requirements within the local organisation's policy.

1. *The name of the Board / EMT accountable person and the RA Manager within the organisation must be named within the policy. The policy needs to outline the governance requirements placed upon these individuals. The local organisation's policy must be updated to reflect any changes to the named individuals.*

    - The responsible officer at Board level will be the Trust Senior Information Risk Owner (SIRO), a role currently under the leadership of Dawn Hanwell, Chief Financial Officer. The SIRO role has overall responsibility for all aspects of information risk, as well has having the ICT and Information Governance functions of the Trust in their portfolio, giving a strategic fit for SmartCard related issues.

    - The Trust RA Manager is *TBC*.

      The RA Manager will monitor and disseminate any relevant information relating to SmartCards and RA issues to appropriate people within the Trust.

    - The Trust Deputy RA Manager is Carl Starbuck – Head of Information Governance. The Deputy RA Manager will also monitor and disseminate any relevant information relating to SmartCards and RA issues to appropriate people within the Trust. The Deputy RA Manager is also the Trust's designated Privacy Officer, and will be responsible for the clearing of SPINE alerts on a daily basis, verifying all access as either being to records of LYPFT service users or alternatively challenging any access outside of this to establish the need for access.

- As the Trust allocates SmartCard permissions via RA interface with ESR, HR / Workforce contacts are operationally responsible for the printing and distribution of SmartCards, and the allocation of permissions to SmartCard users via ESR. Margaret Kershaw & Karen Eason are appropriate contacts in HR / Workforce.

- All staff who hold an NHS SmartCard or alternative access arrangements which act as a virtual SmartCard have a personal responsibility to:-

    - Keep the card safe and secure at all times
    - Keep the PIN code confidential
    - Report it immediately if lost or stolen
    - Not share the SmartCard and / or PIN with anyone else
    - Not allow a logged-on SmartCard to be used by anyone else
    - Only use the systems and data which the SmartCard facilitates access to for their intended legitimate purposes
    - Not abuse the access to systems and data which the SmartCard facilitates.

2. *The policy must describe how access rights will be granted and revoked in a timely way, ensuring that requirements for staff to be able to access electronic records in a timely way can be met and that individuals do not retain access within an organisation once they have left that organisation.*

    - SmartCards will be issued via HR / Workforce as above via new starters presenting with appropriate identification documents at the commencement of employment.
    - Managers will trigger the leavers process via the SW form mechanism, which also triggers the workflow to remove access from Trust systems and to deduct the leave from the Trust's Registration Authority. If the leaver is also leaving the NHS, the manager has a responsibility to also retain and securely destroy the leaver's physical SmartCard.
    - Staff leaving the Trust but remaining in the NHS will retain their SmartCard to use in their next post, if required.

3. *The policy must not contradict the mandatory requirements contained within this national RA Policy. At a minimum the local policy must cover:*

    i. Governance arrangements
    ii. A demonstration of the adherence to this RA Policy requirements in relation to the verification of identity
    iii. Roles & responsibilities
    iv. NHS Smartcard and other approved devices use

The above statements set out our approach to (3). The Trust will follow the NHS National Registration Authority Policy at all times.

4. *The local policy must be formally signed off by the organisation at an appropriately senior level, e.g., the EMT, the IG Committee on a delegated authority basis, etc.*

    - The above policy was ratified by the Trust IG Group, who act with the delegated authority of the SIRO.

Appendix F – National Data Opt-Out Policy

As a provider of NHS services, the Trust is obligated to enact the requirements of the National Data Opt-Out. This appendix sets out our approach to this as a matter of Trust policy, in alignment with National policy.

To comply with national data opt-out policy, we need to put procedures in place to review uses or disclosures of confidential patient information against the operational policy guidance. The Trust and its staff are required to adhere to the operational policy guidance at all times.

Although the NHS delayed the implementation deadline for compliance due to the impact of the COVID-19 pandemic (to 31st July 2022), the Trust had already implemented the Opt-Out, as follows, and will continue to do so as a matter of policy:-

- The Trust will receive & consume the elective Opt-Out choices of our service users from the national MESH service.
- The Trust will hold & process these Opt-Outs in our back-office systems.
- Datasets drawn from our systems for secondary uses will be produced minus those that have opted out, where appropriate.
- Opt-Out choices will NOT be recorded in our core clinical systems (CareDirector etc.), so that staff in service user facing roles will be unaware of their choices such that this does not affect staff's view of the service user.
- If asked, staff should signpost service users to appropriate resources to understand and register their Opt-Out choice. The following websites are appropriate:-

  For information & support for service users & the Opt-Out (including different languages):-

  https://digital.nhs.uk/services/national-data-opt-out/supporting-patients-information-and-resources

  For service users to register an Opt-Out:-

  https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/

PART B

3 IDENTIFICATION OF STAKEHOLDERS

The table below should be used as a summary. List those involved in development, consultation, approval and ratification processes.

Stakeholder	Level of involvement
Information Governance Group (comprising) • Data Protection Officer • IG Support Officer • Chief Information Officer • ICT Service Desk Manager • ICT Support Analyst • Network Manager	Consultation
Staffside representative	Consultation
Information Governance Group	Approval
Policy & Procedure Group	Ratification

4 REFERENCES, EVIDENCE BASE

- Data Protection Act (2018)
- UK General Data Protection Regulation
- Human Rights Act
- Computer Misuse Act
- NHS Confidentiality Code of Practice
- Caldicott Principles
- NHS Records Management Code of Practice
- Professional codes of conduct from the BMA, GMC and NMC and others including Allied Health professionals, Finance Professionals and NHS Managers

5 ASSOCIATED DOCUMENTATION (if relevant)

- IG-0001 – Information Governance Policy
- IG-0002 – Health Records Policy
- IG-0006 – Data Quality Policy
- IG-0007 – Corporate Records Management Guidance
- IG-0008 – Medical Records Subject Access Request Procedure
- IG-0009 – Safe Haven Guidance
- IG-0010 – Data Protection Policy

- IT-0001 – Encryption Policy
- IT-0002 – Internet Use Policy
- IT-0003 – Email Use Policy
- IT-0004 – Network Security Policy

- IT-0005 – Portable Computing Device Policy
- IT-0008 – Information Security Policy
- IT-0009 – Supplier Support Access Agreement Procedure
- IT-0010 – Mobile & Smartphone Communications Policy

- IG Group Terms of Reference

6 STANDARDS/KEY PERFORMANCE INDICATORS (if relevant)

Effectiveness of the policy will be monitored by the number and severity of IG incidents occurring within the Trust, and that the Trust remains free of adverse publicity and punitive sanctions imposed by the Information Commissioner or other regulatory body.

The NHS Digital Data Security & Protection Toolkit scoring will also be viewed as an indicator of performance against this policy and other policy / procedural documents in this area.

7. EQUALITY IMPACT

The Trust has a duty under the Equality Act 2010 to have due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations between people from different groups. Consideration must be given to any potential impacts that the application of this policy/procedure might have on these requirements and on the nine protected groups identified by the Act (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, gender and sexual orientation).

Declaration: The potential impacts on the application of this policy/procedure have been fully considered for all nine protected groups. Through this process I have not identified any potential negative impacts for any of the nine protected groups.

Print name: Carl Starbuck

Job title: Information & Knowledge Manager

Date: 28/10/2022

If any potential negative impacts are identified the Diversity Team must be contacted for advice and guidance: email; diversity.lypft@nhs.net.

CHECKLIST

To be completed and attached to any draft version of a procedural document when submitted to the appropriate group/committee to support its consideration and approval/ratification of the procedural document.

This checklist is part of the working papers.

	Title of document being newly created / reviewed:	Yes / No/
1.	**Title**	
	Is the title clear and unambiguous?	✓
	Is the procedural document in the correct format and style?	✓
2.	**Development Process**	
	Is there evidence of reasonable attempts to ensure relevant expertise has been used?	✓
3.	**Content**	
	Is the Purpose of the document clear?	✓
5.	**Approval**	
	Does the document identify which committee/group will approve it?	✓
6.	**Equality Impact Assessment**	
	Has the declaration been completed?	✓
7.	**Review Date**	
	Is the review date identified?	✓
	Is the frequency of review identified and acceptable?	✓
8.	**Overall Responsibility for the Document**	
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	✓

Name of the Chair of the Committee / Group approving			
If you are assured this document meets requirements and that it will provide an essential element in ensuring a safe and effective workforce, please sign and date below and forward to the chair of the committee/group where it will be ratified.			
Name	*Carl Starbuck*	Date	*28 October 2022*
Name of the chair of the Group/Committee ratifying			
If you are assured that the group or committee approving this procedural document have fulfilled its obligation please sign and date it and return to the procedural document author who will ensure the document is disseminated and uploaded onto Staffnet.			
Name	*Cath Hill*	Date	*10 November 2022*