Blackpool Teaching Hospitals
NHS Foundation Trust

Confidentiality Code of Conduct

Unique Identifier:	CORP/POL/107				
Version Number:	8				
Type of Update / Status:	Ratified with Moderate Changes				
Divisional and Department:	Information Governance Department / Health Informatics				
Author / Originator and Job Title:	Samuel Winter Information Governance Manager				
Replaces:	CORP/POL/107, Version 7.1, Confidentiality Code of Conduct				
Description of amendments:	Moved to New Template Updates to Send Secure process Inclusion of National Data Opt Out and the Data Protection Principles information General review Policy listings updated				
Approved by:	Health Informatics Committee				
Approved Date:	18/08/2021				
Issue Date:	18/08/2021				
Review Date from Date of Approval:	1 Year ☐	2 Years ☐	3 Years ☒ 18/08/2024	4 Years ☐	5 Years ☐

Version Control Sheet

This must be completed and form part of the document appendices each time the document is updated and approved

Date dd/mm/yy	Version	Author	Reason for changes
18/08/21	8	Samuel Winter, Information Governance Manager	See above for description of amendments

Consultation / Acknowledgements with Stakeholders

Name	Designation	Date Response Received
Hayley Atkinson	Head of Information Governance	10/06/2021
Patricia Butcher	Data Protection Officer	10/06/2021
Melanie Baines	Information Governance Specialist	11/06/2021

CONTENTS

1 Introduction / Purpose

The Trust is committed to safeguarding the confidentiality of the individual and the information it holds about them.

This Policy has been produced to:

- Lay down the principles that must be observed by all staff and contractors who work within Blackpool Teaching Hospitals and have access or come in to contact with person-identifiable information / confidential information.
- Inform staff of the need and reasons for keeping information confidential.
- Inform staff about what is expected of them.
- Ensure the use and sharing of information complies with our legal responsibilities.
- Protect the Trust as an employer and as a user of confidential information.

2 General Principles / Target Audience

This policy / guidance document applies to all employees of the Trust including agency staff, honorary contractors other commercial third-party contractors and volunteers.

3 Definitions and Abbreviations

DPO	Data Protection Officer
GAG	Confidentiality Advisory Group
GDPR	General Data Protection Regulation
HR	Human Resources
ICO	Information Commissioners Office
IGM	Information Governance Manager
NDO	National Data Opt Out
PID	Person Identifiable Data
SIRO	Senior Information Risk Owner

4 Policy

4.1 Introduction

All employees working in the NHS are bound by a legal duty of confidence to protect the personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within:

- The Data Protection Act 2018 (1)
- The Data Protection Principles (see Appendix 2)
- General Data Protection Regulation (GDPR)
- The Common Law Duty of Confidence.
- The NHS Care Record Guarantee.

- Professional Codes of Conduct.
- Caldicott Principles (see Appendix 1).
- The NHS Confidentiality Code of Practice (2).
- Freedom of Information Act 2000 (3).
- The Computer Misuse Act (1990).
- Human Rights Act (1998).
- Regulation of Investigatory Powers Act 2000 (4).
- National Health Service Act (2006) (5).
- The Information Security Management NHS Confidentiality Code of Practice (6).

The Confidentiality NHS Code of Practice further endorses this by providing a guide (Appendix 1 Caldicott Principles) to required practice for those who work within or under contract to any NHS organisation.

It is important that Blackpool Teaching Hospitals safeguards the person identifiable and confidential business information that it gathers / creates / processes and discloses in accordance with the law. There are relevant NHS mandatory requirements to provide assurance to patients and the public.

This policy sets out the individual obligations placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

4.2 Definition of Person Identifiable Data (PID)

PID is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

In addition to PID, staff must be aware that extra precautions must be taken when dealing with sensitive personal data.

4.2.1 Definition of Special Categories of Personal Data

Special Categories of Personal Data as defined by the General Data Protection Regulation is personal data which is more sensitive, consisting of information such as:

- racial or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature
- trade union membership
- genetic / biometric or mental health

- sex life / orientation
- commission or alleged commission of any offence
- proceedings for any offence committed or alleged to have been committed

4.2.2 Confidential Information – Personal and Non-Personal

Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

Patients have a right to expect that a doctor, nurse or other members of the Health / Social Care Team or Trust staff in general will not disclose any personal information gathered during the course of their duties, unless permission is given. Without assurances about confidentiality patients may be reluctant to give information that may be required in order to provide care.

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, including temporary staff.

Non identifiable information can also be classed as confidential and personal e.g. confidential business information such as financial reports, commercially sensitive information, contracts, trade secrets, procurement information, which must also be treated with the same degree of care.

Confidential information may be known or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally. Information that identifies individuals personally must be assumed to be confidential and should not be accessed or used unless absolutely necessary. Whenever possible, anonymised data (from which personal details have been removed and which therefore cannot identify the individual) is to be used instead. Note however that even anonymised information can only be used for justified purposes.

4.3 Roles and Responsibilities

No employee shall knowingly access or misuse any information or allow others to do so without appropriate authorisation. Any breaches / potential breaches of confidence are to be reported in accordance with the Management of Incidents, Incorporating Serious Incidents (CORP/POL/605 (7)).

4.3.1 The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that NHS England policies comply with all legal, statutory and good practice guidance requirements.

4.3.2 The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

4.3.3 The National Data Guardian

The national Data Guardian is appointed by the Government and chairs a panel of experts in an independent advisory capacity. It works with bodies such as The National Data Guardian and NHS England to implement recommendations from The Dame Fiona Caldicott review: 'Information: to share or not to share'

4.3.4 Data Protection Officer

In compliance with GDPR, we are required to appoint a Data Protection Officer; part of their role is to monitor compliance within the Trust, offer advice and co-operate with the ICO as their main point of contact.

4.3.5 The SIRO Structure

The SIRO (Senior Information Risk Owner) structure is implemented throughout the Trust. It consists of a senior group of staff within the organisation who manage systems and access to information. It uses a risk methodology to ensure any risks or potential breaches of confidentiality are identified and managed. Usually any breaches of confidentiality will be investigated by one or more persons identified within the SIRO Structure. More detailed information can be found by looking at the Information Governance Framework (CORP/POL/065 (8)).

4.3.6 Director with responsibility for Human Resources (HR)

The Director with responsibility for HR is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate inductions for all staff.

4.3.7 Managers

Managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information within individual areas e.g. wards, departments. Managers must also ensure supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Trust Incident Reporting System.

4.3.8 The Information Governance Manager (IGM)

The IGM is responsible for maintaining the currency of this policy, providing advice on request to any member of staff on the issues covered within it.

4.3.9 Individual Employees

All employees are responsible for maintaining confidentiality. This duty of confidentiality is written into all employment contracts. Unauthorised access of information gained, either directly or indirectly in the course of one's duty will be considered a disciplinary offence that could result in dismissal.

Individuals are:

- Authorised only to have access to the personal information they need to know in order for them to perform their duties. Unauthorised access or attempting to gain access to information for any other purpose is a breach of confidentiality as is passing information on to someone who is not authorised to receive it.
- Responsible for safeguarding the confidentiality of all personal and Trust information to which they have access, this includes its safe transfer and storage.
- Personally responsible for any decision to pass on information to another person / third party.
- Responsible for adhering to the Confidentiality NHS Code of Conduct, Caldicott Principles, the Data Protection Act 2018 (1), the UK General Data Protection Regulation (GDPR (9)) and the Freedom of Information Action 2000 (3).
- Also expected to treat any non-person identifiable information that could be considered sensitive to the business of the Trust with the same degree of care as would be afforded to person identifiable information.
- Required to read and sign this policy confirming their understanding at the start of employment with the Trust and at least annually thereafter see Appendix 4 and 5 (Form and Code will be included in the "New Starter" pack).

4.3.10 Acting on a duty of Confidentiality

Any personal information, non-clinical or clinical, must be treated as confidential.

No personal information, given or received in confidence, may be passed to another person or organisation without the consent of the provider of the information. This is usually the patient but sometimes another person may be the source (e.g. relative or carer).

No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.

Whilst patients usually understand and accept that information may be shared within the health care team in order to provide their care, it is still necessary to check that the patient understands what will be disclosed and who may be contributing to their care. All healthcare professionals providing care / treatment must ensure they communicate clearly how information is to be shared and used each time they talk to the patient. Patients have the right under The NHS Constitution - Respect, Consent and Confidentiality to:

- Be informed about how their information is used.
- Request that their confidential information is not used beyond their own care and treatment (and to have any objections considered where their wishes cannot be followed).

It is also important to respect the wishes of any patient who objects to their information being shared, except where this would put others at risk of death or serious harm.

The overriding principle is that patients should not be shocked to find out how their information has or is being used or shared, rather that they should be effectively informed to allow them to exercise their rights in relation to their data.

The duty of confidentiality owed to a deceased patient is to be viewed as being consistent with the rights of living individuals.

4.3.11 The Use of mobile devices in hospitals (phones, tablets and cameras) - Privacy and Dignity

The use of mobiles devices should be kept to a minimum and must only be used where allowed. Users of mobile devices must be considerate of patient privacy and dignity and their common law duty of confidentiality.

Video / photographs of patients must not be taken on phones or any other device by patients or visitors without the nurse in charge agreement.

Patients may keep a record of their own care but should inform staff in advance and must have regard to the privacy and dignity of others.

The same care and attention applies to recording conversations.

For more information please see Appendix 3 and also refer to the Use of Personal Mobile Devices and Social Media / Social Networking Policy (CORP/POL/220 (10))

4.3.12 When information can be disclosed

Information can be disclosed under the following circumstances:

- When anonymised. The removal of **all** identifiers (including metadata) which would enable re-identification of the data subject.
- When the information is required by law or under a court order. In this situation staff must contact the Data Access Team on **ext. 53056** or by email using bfwh.data.access@nhs.net alternatively contact the Information Governance Helpline on **ext. 53057** or the IG inbox by using bfwh.information.governance@nhs.net for advice and approval before disclosing.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or,

- With support of a Section 251 of the National Health Service Act (5) and its current regulations the Health Service (Control of patient information) regulations 2002 (11).

  Section 251 was introduced because it was recognised that there were essential activities of the NHS, and important medical research, that required the use of identifiable patient information but, because patient consent had not been obtained to use people's personal and confidential information for these other purposes, there was no secure basis in law for these uses. Section 251 was established to enable the common law duty of confidentiality to be overridden to enable disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent was not practical, having regard to the cost and technology available. See more at: https://www.legislation.gov.uk/ukpga/2006/41/section/251

  A Section 251 can only be granted by the Confidentiality Advisory Group (CAG)

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must not disclose information unless they have been informed by their line manager of an approved policy / procedure relevant to their area of work e.g. Safeguarding Team, Health Visitors. In all other cases, guidance must be sought from the Information Governance Department.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with the Information Governance Team and refer to the Procedure for releasing information to the Police (CORP/POL/555 (12)).
- In the case of an in-patient or their representative asking to view their information whilst they are on the ward. It is possible for the ward staff to allow the patient to view the current episode of care as long as the Consultant in charge of the care has given his / her approval. Approval must be recorded in the hospital case notes. Patients / representatives must not be left alone with the information and a member of staff must be present. Members of staff are not obliged to comment throughout the viewing but if a patient does not understand the information, medically qualified staff may provide assistance. If the patient has multiple episodes of care, permission must first be sought form the relevant health professionals before being allowed to view. Usually this is not possible to administer whilst the person is an in-patient and therefore it must be referred to the Data Access Team.
- In adherence with the requirements of the National Data Opt Out (NDO). The NDO allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning. See more at: National data opt-out - NHS Digital (13)

4.3.13 Additional safeguards when sharing information

As a general rule, do not give out personal information unless you are sure that the person requesting it has a legitimate need to see it. Consider the person to whom the information refers, do they know and have they consented to the information being passed on if not then it is unlikely that it is appropriate to pass the information to a third party.

If you have any concerns about disclosing or sharing personal information you must discuss them with your Line / Senior Manager, the On-Call Duty Manager or the Information Governance Department. If you cannot find anyone at the time to help, then wait to release the information until you are satisfied that the disclosure can take place.

Remember that under current law, no-one but the patient can make decisions about sharing their health information but them unless:

- It is within their vital interests; and,
- They are deemed unable to make such decisions for themselves i.e. they are considered to "lack capacity" under the terms of the Mental Capacity Act (14).

A senior health care professional involved in the patient's care may consider it to be in the patients' best interests to share information. This judgment should take account of the views of relatives and carers, and previous views expressed (recorded) by the patient.

In order to provide health care for a patient the care team may need to include people from other services, such as social services or education ensure the patient is informed about who you are sharing their information with. If it is necessary to share patient information with organisations outside the NHS, ensure the patient agrees to this before it takes place. If the patient has any concerns about this discuss with them any possible effect this may have on their care and alternatives available to them.

Remember that just as a patient may give their consent to share their information, they may also request that no further information is shared. However, this may compromise their care and a documented conversation around this should be held.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails and surface mail.

Before sending any sensitive or confidential information by email, including information about patients or staff, it is important to ensure the following:

- There is a legitimate purpose for sending the information
- Only the minimum necessary amount of information is going to be used
- Each intended recipient has a legitimate right to see the information
- No person-identifiable information is included in the subject line

Transferring patient information by email to anyone outside Blackpool Teaching Hospitals network may only be undertaken by using 'send secure' (this encrypts the email) or through an exchange within the NHS Mail system (i.e., from one NHS.net account to another NHS.net account or to a secure government domain e.g., gsi.gov.uk), since this ensures that mandatory government standards on encryption are met.

You can encrypt an email by entering [secure] in square brackets in the subject line.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent (this must be recorded) and the information is **not** person-identifiable or confidential information.

See Section 5 for further guidance and Polices.

4.3.14 Requests for information

The Data Access Team are available on **ex 53056** or by email using bfwh.data.access@nhs.net during normal office hours to assist you with responding to requests for information and dependant on the circumstances facilitate the response for / with you. Out of hours you must refer to your local departmental procedures.

4.3.15 Telephone enquiries

If a request for information is made by telephone the rules above still apply:

- Always check the identity of the caller.
- Confirm that they are entitled to the information they request.
- If necessary, take a number, verify the request independently and call back.

Remember even the fact that a person is a patient in hospital is confidential and they may not wish for their information to be disclosed.

If in doubt consult your Line or Senior Manager.

4.3.16 Requests for information by the Police

The Police do not have an automatic right to information about an individual. If you do receive a request from the Police refer it to the Data Access Team or Duty Site Manager. You can find further guidance in the 'Information Sharing Policy' (CORP/POL/555 (12))

4.3.17 Requests for information by the Media

Do not give out any information to members of the press etc. If you receive any request from the media either by personal visit or by phone refer the person to the Trusts' Communications Department.

4.3.18 Working away from the office environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry Trust information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

Taking home / removing paper documents that contain person-identifiable or confidential information from Trust premises is discouraged.

When working away from the Trust locations staff must ensure that their working practice complies with Trust policies and procedures. Any removable media must be encrypted as per the current Trust Encryption Procedure (15).

To ensure safety of confidential information staff must always keep it on their person whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations

Staff must minimise the amount of person-identifiable information that is taken away from Trust premises.

If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of Trust buildings.
- Confidential information is kept out of sight whilst being transported.
- If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends / colleagues must not be able to see the content or have any access to the information.
- Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person identifiable or confidential information on a privately owned computer device.

For Further Information please see the 'Transportation of Person Identifiable information and Trust sensitive information in paper form, electronic devices and dictation tapes 'Procedure, (CORP/PROC/467 (16)).

4.3.19 Storage of information

Information must not be stored on removable media unless it is encrypted as per the Trust Encryption Procedure (CORP/PROC/509 (15)) and the Mobile Device Management Policy (CORP/POL/513 (17)).

Information may be held on paper but must be kept under secure conditions e.g.

- Locked filing cabinets.
- Fob locked office.
- Digi locked room.
- Password protected system.

4.3.20 Disposal of information

When you dispose of paper-based person-identifiable information or confidential information always use a 'Confidential Wastepaper Bin' or 'Confidential Waste' sacks. You can request a collection from compass Medirest on **ext. 55989**. Upon collection additional white bags will be replaced. Keep the waste in a secure place until it can be collected for secure disposal.

All identifiable and confidential information no longer required must be deleted/disposed of in accordance with the 'Records Management: Code of Practice for Health and Social Care' retention periods (18).

For more information on retention and disposal of information please contact the Information Governance Department.

4.3.21 Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and must not divulge information accidentally. Staff may be held personally liable for a breach of confidence and have an obligation not to:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.
- Use someone else's password to gain access to information.
- Allow anyone else to use their password.

Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in dismissal.

4.3.22 Abuse of privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018 (1).

4.3.23 Confidentiality Audits and Monitoring

Good practice requires all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Information Governance team through a programme of audits.

It is important that staff are reminded of monitoring. Staffs actions are monitored and audited within systems. This ensures:

- The integrity of our data processing is upheld.
- We are meeting our legal requirements
- We use the data to improve our service/systems

The Information Security Officer will provide regular reports to the Information Governance Risk and Assurance Group (IGRAG). The number of reported "information" untoward incidents including:

- Confidentiality
- Security
- Misuse of Data
- Staff training undertaken

4.3.24 Training and Awareness

Training and awareness is the importance of the maintenance of confidentiality and information security. It will be an ongoing process throughout an individual's employment with the Trust and will form part of the mandatory training programme.

It will be provided via a number of methods supplied / supported by the Information Governance Department including:

- Trust Induction
- Mandatory update sessions
- E-learning package
- Confidentiality and information Security training sessions
- On-going awareness campaign

Managers will be responsible for ensuring that employees are made aware of any specific ward / departmental requirements/procedures.

4.3.25 Distribution and Implementation

This document will be made available to all staff via the Trust Document Library on the intranet site.

All staff will be required to sign to say they have read and understood the policy at induction and thereafter annually as part of the appraisal process.

5 References and Associated Documents

1. **Crown.** Data Protection Act 2018. [Online] 2018. [Cited: 16 06 2021.] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

2. **Department of Health and Social Care.** Confidentiality: NHS Code of Practice. [Online] Published: 07/11/2003. [Cited: 07 04 2021.] https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice.

3. **Crown.** Freedom of Information Act 2000. [Online] 2000. [Cited: 10 05 2021.] http://www.legislation.gov.uk/ukpga/2000/36/contents.

4. —. Regulation of Investigatory Powers Act 2000. [Online] 2000. [Cited: 21 06 2021.] https://www.legislation.gov.uk/ukpga/2000/23/contents.

5. —. National Health Service Act 2006. [Online] 2006. [Cited: 25 06 2021.] https://www.legislation.gov.uk/ukpga/2006/41/contents.

6. **Department of Health and Social Care.** Information Security Management: NHS Code of Practice. [Online] 20 04 2007. [Cited: 21 06 2021.] https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice.

7. **BTHFT - Policy.** Management of Incidents, Incorporating Serious Incidents. [Online] 22 12 2020. [Cited: 12 05 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-605.docx. CORP/POL/605.

8. —. Information Governance Framework Policy 2019-2021. [Online] 09 07 2019. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-065.docx. CORP/POL/065.

9. **Information Commissioners Office.** Guide to the UK General Data Protection Regulation (UK GDPR). [Online] [Cited: 21 06 2021.] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

10. **BTHFT - Policy.** The Use of Personal Mobile Devices and Social Media / Social Networking. [Online] 23 11 2018. [Cited: 26 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-220.docx. corp/pol/220.

11. **Crown.** The Health Service (Control of Patient Information) Regulations 2002. [Online] 2002. [Cited: 26 08 2021.] https://www.legislation.gov.uk/ukdsi/2002/0110398904/contents.

12. **BTHFT - Policy.** Information Sharing Policy – Personal Information. [Online] 08 04 2020. [Cited: 11 05 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-555.docx. CORP/POL/555.

13. **NHS Digital.** National data opt-out. [Online] [Cited: 26 08 2021.] https://digital.nhs.uk/services/national-data-opt-out.

14. **Crown.** Mental Capacity Act 2005. [Online] 2005. [Cited: 19 03 2021.] https://www.legislation.gov.uk/ukpga/2005/9/contents.

15. **BTHFT - Procedure.** Encryption. [Online] 18 08 2021. [Cited: 26 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-PROC-509.docx. CORP/PROC/509.

16. —. Transportation of Person Identifiable information and Trust Sensitive information in paper form, electronic devices, dictation tapes and IT Backup Media. [Online] 14 06 2021. [Cited: 25 06 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-PROC-467.docx. CORP/PROC/467.

17. **BTHFT - Policy.** Mobile Computing Equipment Management (Mobile Devices and Media). [Online] 09 05 2018. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-513.docx. CORP/POL/513.

18. **NHS Digital.** Records Management Code of Practice. [Online] 04 08 2021. [Cited: 26 08 2021.] https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/.

19. **National Data Guardian.** Caldicott review: information governance in the health and care system. [Online] 26 04 2013. [Cited: 26 08 2021.] https://www.gov.uk/government/publications/the-information-governance-review.

20. **BTHFT - Policy.** Records Management Policy Manual. [Online] 2018. [Cited: 26 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-054.docx. CORP/POL/054.

21. **BTHFT - Procedure.** Retention, Disposal and Destruction of Community Health Record Folders. [Online] 23 07 2018. [Cited: 26 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-PROC-713.docx. CORP/PROC/713.

22. **BTHFT - Policy.** Access Control – Information Systems (electronic). [Online] 18 08 2021. [Cited: 26 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-508.docx. CORP/POL/508.

23. —. Information Security Policy. [Online] 09 06 2021. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-178.docx. CORP/POL/178.

24. —. Data Protection. [Online] 13 02 2019. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-064.docx. CORP/POL/064.

25. —. Email Policy, including Instant Messaging (IM). [Online] 18 08 2021. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-068.docx. CORP/POL/068.

26. —. Health Informatics Information Security and Information Technology (IT) Serious Incident Reporting and Monitoring. [Online] 14 08 2019. [Cited: 25 08 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-172.docx. CORP/POL/172.

27. **Crown.** Computer Misuse Act 1990. [Online] 1990. [Cited: 21 06 2021.] https://www.legislation.gov.uk/ukpga/1990/18/contents.

28. —. Human Rights Act 1998. *Article 8.* [Online] 1998. [Cited: 28 07 2021.] https://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7.

29. **BTHFT - Policy.** Freedom of Information Act 2000 and Environmental Information Regulations 2004. [Online] 09 07 2019. [Cited: 22 06 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-POL-106.docx. CORP/POL/106.

30. **BTHFT - Guideline.** Implementing the Mental Capacity Act 2005 and Apply the Supporting Code of Practice. [Online] 26 11 2019. [Cited: 26 04 2021.] http://fcsp.xfyldecoast.nhs.uk/trustdocuments/Documents/CORP-GUID-083.docx. CORP/GUID/083.

31. **National Data Guardian.** UK Caldicott Guardian Council. [Online] [Cited: 26 08 2021.] https://www.gov.uk/government/groups/uk-caldicott-guardian-council#Manual-for-Caldicott-Guardians.

32. —. Health and Care Review of Data Security Consent and Opt-Outs. [Online] 06 2016. [Cited: 26 08 2021.] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF.

33. **Crown.** The Common Law Duty of Confidentiality. [Online] [Cited: 25 08 2021.] http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173.

34. **Department of Health and Social Care.** NHS Constitution for England. [Online] Last Updated: 01/01/2021. [Cited: 19 03 2021.] https://www.gov.uk/government/publications/the-nhs-constitution-for-england.

Appendix 1: Caldicott Principles

The term Caldicott refers to a review commissioned by the Chief Medical Officer in 1997 under the chairmanship of Dame Fiona Caldicott. They investigated ways in which patient information is used in the NHS.

The Information Governance Review (19), known as Caldicott 2, was carried out in 2014. As a result of this review a seventh principle was added.

1. **Justify the purpose(s) -** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary -** Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary personal confidential data -** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis -** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. **Everyone with access to personal confidential data should be aware of their responsibilities -** Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Comply with the law -** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality -** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employer.

Appendix 2: The Data Protection Principles

Article 5 of the UK GDPR sets out seven key Data Protection Principles which lie at the heart of the general data protection regime and our approach to processing personal data.

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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

Appendix 3: The Use of mobile devices in clinical areas

THE USE OF MOBILE DEVICES SHOULD BE KEPT TO A MINIMUM AND MUST ONLY BE USED WHERE ALLOWED.
USERS OF MOBILE DEVICES MUST BE CONSIDERATE OF PATIENT PRIVACY, DIGNITY AND NEED FOR QUIET

Area	Designation	Staff	Patients	Visitors
Intensive Care / High Dependency Units Operating Theatres and Recovery Areas Neonatal Units Emergency / Resuscitation Areas Renal Dialysis Units Delivery Rooms	Prohibited	Mobile device cameras can only be used for urgent clinical photographs. Phones can be used for work purposes or during breaks in a permitted area. Staff with carer responsibilities should agree a landline contact with their line manager	**Not allowed** The Nurse in Charge can agree exceptional patient use for those with specific communication or carer needs or for those confined to bed areas. Care should be taken to avoid	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building. The Nurse in Charge can agree exceptional use
Other clinical areas (not in prohibited list) that the Trust has designated as restricted due to risks outweighing the benefits to patients and visitors	Restricted	Mobile device cameras can only be used for urgent clinical photographs. Phones can be used for work purposes or during breaks in a permitted area. Staff with carer responsibilities should agree a landline contact with their line manager	**Not allowed** The Nurse in charge can agree exceptional patient use as above but this should avoid proximity electronic Medical Device e.g. on Maternity Units pictures can be taken of newborn babies if this is the ONLY method of taking the picture	**Not allowed** Visitors should leave the area. Calls must only be made from a permitted area or outside the building The Nurse in Charge can agree exceptional use
Other areas e.g. waiting areas	Permitted	**Allowed,** but no personal use when on duty (Phones can be used in breaks).	**Allowed** but please have regard to others and try to keep a distance from electronic medical devices. Phones should not be used between 23:00 and 07:00 hours. If using video chat the camera must be facing you and you need to be aware that you may pick up other people's conversations and other people may hear both sides of your conversation. Please Respect staff and service user privacy and dignity when updating your status on any social media sites / apps.	

VIDEO / PHOTOGRAPHS OF PATIENTS MUST NOT BE TAKEN ON PHONES BY PATIENTS OR VISITORS WITHOUT NURSE IN CHARGE AGREEMENT. KEEPING A RECORD OF YOUR OWN CARE IS PERMITTED BUT PLEASE INFORM STAFF IN ADVANCE AND HAVE REGARD TO THE PRIVACY AND DIGNITY OF OTHERS

Appendix 4: Data Protection and Confidentiality Code of Conduct - Employee

Blackpool Teaching Hospitals
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY CODE OF CONDUCT

I understand that as an employee of the Trust I am bound by a legal duty of confidence to protect any personal information that I come into contact with during the course of my work. I also understand that I am also expected to treat any non-person identifiable information that could be considered sensitive to the business of the Trust with the same degree of care.

I will not at any time during my employment or afterwards disclose to any person / organisation (including distributors, firms or companies otherwise connected with the Trust):

- Personal Information regarding patients (including prospective patients), staff (in connection with their employment).
- Corporate information relating to the business, dealings, accounts, finances, trading, software, know-how, affairs of the Trust.

Unless I have the authority to do so and only within the confines of the Law and local Trust Policy, Procedure and Guidance. This includes but is not limited to:

- The Data Protection Act 2018
- General Data Protection Regulation
- The Freedom of Information Act 2000
- The Human Rights Act 2000
- The Computer Misuse Act 1990
- Crime and Disorder Act 1998
- The Access to Health Records Act 1990
- Access to Medical Reports Act 1998
- Confidentiality Code of Conduct Policy (CORP/POL/107)

All notes, memoranda, records and other documents created/used by me during the course of my duties for the Trust shall remain the property of the Trust and shall be handed over by me to the Trust from time to time on demand and, in any event, upon termination of my employment.

I understand that systems are monitored and regular audits are conducted.

I understand that any breach of this Code of Conduct may constitute a disciplinary offence that could result in disciplinary action being taken. The outcome of such action could be regarded as gross misconduct and lead to dismissal. Any breach of this Code of Conduct after my employment has ended may result in legal action being taken.

I understand my role and responsibilities in relation to the protection of both manual and automated data.

I understand my responsibilities in relation to data confidentiality.

I have read the Confidentiality Code of Conduct Policy and Guidance.

Print Name .....

Sign name..... Date.....

Line Manager – A verbal explanation of the above statement has been provided to the above member of staff.

Signature of Line Manager .....

Date .....

Appendix 4: Data Protection and Confidentiality Code of Conduct - Employee

NHS
Blackpool Teaching Hospitals
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY CODE OF CONDUCT

Relevant Acts of Parliament and NHS guidelines and what they mean for employees			
Requirement	**What it covers**	**Personal responsibilities**	**Penalties for breaches**
Data Protection Act 2018	Person identifiable information about living individuals – manual and automated records (e.g. on computer, video tape, digital images)	Keep all person identifiable information secure and confidential – see Code of Conduct for specific details	Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant
General Data Protection Regulation	Dealing with special category personal data	As above	As above
Human Rights Act 1998 (Article 8)	An individual's right to privacy for themselves and their family members	As above	As above
Computer Misuse Act 1990	Unauthorised access to computer held programs and information/data	Do not use any other persons access rights (e.g. user id and password) to access a computer database	A criminal record and a prison sentence of up to 5 years
Common Law of confidentiality	An individual's right to confidentiality of their information when alive and once they have died	Keep all information secure and confidential. Also remember this covers wishes of deceased persons – if it is recorded they do not want details of their treatment disclosed when they die this wish will normally need to be respected	Disciplinary action
Caldicott	Security and confidentiality of personal health and social care information for patients and service users	See Code of Conduct and further information available from the A/T/P Caldicott Guardian	Disciplinary action
Contract of employment	Employees responsibilities including security and confidentiality of any information accessed during the course of work	Comply with contract and Code of Conduct	Disciplinary action

A completed copy of this form is to be kept in the personal file of each member of staff.

Advice and assistance in relation to Data Protection and Confidentiality issues can be sought from the Information Governance Department.

Appendix 5: Data Protection and Confidentiality Code of Conduct – Agency Member of staff

Blackpool Teaching Hospitals
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY CODE OF CONDUCT- AGENCY MEMBER OF STAFF

I understand that working as an Agency member of staff for the Trust I am bound by a legal duty of confidence to protect any personal information that I come into contact with during the course of my work. I also understand that I am expected to treat any non-person identifiable information that could be considered sensitive to the business of the Trust with the same degree of care.

I will not at any time during my employment or afterwards disclose to any person / organisation (including distributors, firms or companies otherwise connected with the Trust):

- Personal Information regarding patients (including prospective patients), staff (in connection with their employment).
- Corporate information relating to the business, dealings, accounts, finances, trading, software, know-how, affairs of the Trust.

Unless I have the authority to do so and only within the confines of the Law and local Trust Policy, Procedure and Guidance. This includes but is not limited to:

- The Data Protection Act 2018
- General Data Protection Regulation
- The Freedom of Information Act 2000
- The Human Rights Act 2000
- The Computer Misuse Act 1990
- Crime and Disorder Act 1998
- The Access to Health Records Act 1990
- Access to Medical Reports Act 1998
- Confidentiality Code of Conduct Policy (CORP/POL/107)

All notes, memoranda, records and other documents created/used by me during the course of my duties for the Trust shall remain the property of the Trust and shall be handed over by me to the Trust from time to time on demand and, in any event, upon end of the agreed term of the contract.

I understand that systems are monitored and regular audits are conducted.

I understand that any breach of this Code of Conduct may constitute a disciplinary offence that will be reported to my Employment Agency and could result in disciplinary action being taken. The outcome of such action could be regarded as gross misconduct and lead to dismissal. Any breach of this Code of Conduct may result in legal action being taken.

I understand my role and responsibilities in relation to the protection of both manual and automated data.

I understand my responsibilities in relation to data confidentiality.

I have read the Confidentiality Code of Conduct Policy and Guidance.

Print Name .....

Sign name..... Date.....

Line Manager – A verbal explanation of the above statement has been provided to the above member of staff.

Signature of Line Manager .....

Date .....

Appendix 5: Data Protection and Confidentiality Code of Conduct – Agency Member of staff

Blackpool Teaching Hospitals NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY CODE OF CONDUCT- AGENCY MEMBER OF STAFF

Relevant Acts of Parliament and NHS guidelines and what they mean for employees			
Requirement	**What it covers**	**Personal responsibilities**	**Penalties for breaches**
Data Protection Act 2018	Person identifiable information about living individuals – manual and automated records (e.g. on computer, video tape, digital images)	Keep all person identifiable information secure and confidential – see Code of Conduct for specific details	Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant
General Data Protection Regulation	Dealing with special category personal data	As above	As above
Human Rights Act 1998 (Article 8)	An individual's right to privacy for themselves and their family members	As above	As above
Computer Misuse Act 1990	Unauthorised access to computer held programs and information/data	Do not use any other persons access rights (e.g. user id and password) to access a computer database	A criminal record and a prison sentence of up to 5 years
Common Law of confidentiality	An individual's right to confidentiality of their information when alive and once they have died	Keep all information secure and confidential. Also remember this covers wishes of deceased persons – if it is recorded they do not want details of their treatment disclosed when they die this wish will normally need to be respected	Disciplinary action
Caldicott	Security and confidentiality of personal health and social care information for patients and service users	See Code of Conduct and further information available from the A/T/P Caldicott Guardian	Disciplinary action
Contract of employment	Employees responsibilities including security and confidentiality of any information accessed during the course of work	Comply with contract and Code of Conduct	Disciplinary action

A completed copy of this form is to be kept in the personal file of each member of staff.

Advice and assistance in relation to Data Protection and Confidentiality issues can be sought from the Information Governance Department.

Appendix 6: Equality Impact Assessment Form

Department	Information Governance	**Service or Policy**	Policy	**Date Completed:**	06/05/2021

GROUPS TO BE CONSIDERED

Deprived communities, homeless, substance misusers, people who have a disability, learning disability, older people, children and families, young people, Lesbian Gay Bi-sexual or Transgender, minority ethnic communities, Gypsy/Roma/Travellers, women/men, parents, carers, staff, wider community, offenders.

EQUALITY PROTECTED CHARACTERISTICS TO BE CONSIDERED

Age, gender, disability, race, sexual orientation, gender identity (or reassignment), religion and belief, carers, Human Rights and social economic / deprivation.

QUESTION	**RESPONSE**		**IMPACT**	
	Issue	Action	Positive	Negative
What is the service, leaflet or policy development? What are its aims, who are the target audience?	See Purpose			
Does the service, leaflet or policy/ development impact on community safety • Crime • Community cohesion	No			
Is there any evidence that groups who should benefit do not? i.e. equal opportunity monitoring of service users and/or staff. If none/insufficient local or national data available consider what information you need.	No			
Does the service, leaflet or development/ policy have a negative impact on any geographical or sub group of the population?	No			
How does the service, leaflet or policy/ development promote equality and diversity?	No			
Does the service, leaflet or policy/ development explicitly include a commitment to equality and diversity and meeting needs? How does it demonstrate its impact?	No			
Does the Organisation or service workforce reflect the local population? Do we employ people from disadvantaged groups	No			
Will the service, leaflet or policy/ development i. Improve economic social conditions in deprived areas ii. Use brown field sites iii. Improve public spaces including creation of green spaces?	No			
Does the service, leaflet or policy/ development promote equity of lifelong learning?	No			
Does the service, leaflet or policy/ development encourage healthy lifestyles and reduce risks to health?	No			
Does the service, leaflet or policy/ development impact on transport? What are the implications of this?	No			
Does the service, leaflet or policy/development impact on housing, housing needs, homelessness, or a person's ability to remain at home?	No			
Are there any groups for whom this policy/ service/leaflet would have an impact? Is it an adverse/negative impact? Does it or could it (or is the perception that it could exclude disadvantaged or marginalised groups?	No			

Appendix 6: Equality Impact Assessment Form

Does the policy/development promote access to services and facilities for any group in particular?	No			
Does the service, leaflet or policy/development impact on the environment • During development • At implementation?	No			

ACTION:

Please identify if you are now required to carry out a Full Equality Analysis	**Yes**	**No**	**(Please delete as appropriate)**

Name of Author: **Signature of Author:**	Samuel Winter	**Date Signed:**	11/05/2021
Name of Lead Person: **Signature of Lead Person:**		**Date Signed:**	
Name of Manager: **Signature of Manager**	Hayley Atkinson	**Date Signed:**	10/06/2021