CODE OF CONDUCT FOR EMPLOYEES IN RESPECT OF CONFIDENTIALITY

Author:	Rachel Adams, Information Governance Officer
Document Owner:	Sheila Murphy, Trust Secretary and Director of Corporate compliance and Legal service and Data Protection Officer
Revision No:	5
Document ID Number	OTCGR004
Approved By:	Information Governance Group
Implementation Date:	May 2018
Date of Next Review:	May 2020

Code of Conduct for Employees in Respect of Confidentiality

Document Control / History	
Revision No	**Reason for change**
1	Annual Review and update into new format
2	Review and update
3	Two-yearly review and update
4	Two-yearly review and update, additional Caldicott Guardian guideline, change of job titles and organisational names. Storage must be encrypted.
5	Two-yearly review and update. GDPR compliance.

Consultation
Virtual Information Governance Group May 2018.

Code of Conduct for Employees in Respect of Confidentiality

Table of Contents

Code of Conduct for Employees in Respect of Confidentiality

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 All individuals working in the NHS, including contracted employees, non-contract workers such as bank staff, agency staff, volunteers, locums, students and, suppliers (including e.g. window cleaners, maintenance engineers) are bound by legal duties of confidence and to protect personal information they may come into contact with during the course of their work. This is not just a requirement under their contracts with the NHS but also a requirement within the NHS Code of Practice on Confidentiality (November 2003), the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and, in the case of healthcare professionals, professional Codes of Conduct.

1.2 Patients entrust us with sensitive information relating to their health and other matters as part of their treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and use their information appropriately.

1.3 This means that employees are obliged to keep any person identifiable information (e.g. patient and employee records) strictly confidential. It should be noted that employees also come into contact with non-person identifiable information e.g. confidential business information, which should also be treated with the same degree of care.

1.4 Patients generally have the right to understand the way in which their confidential information is being used and in some cases can object to the use of their information. Patients need to be made aware of this right. All 8 Individuals' Rights under the GDPR and DPA are communicated to patients under our Privacy Notice which can be found https://www.medway.nhs.uk/about-us/privacy-policy.htm and the Trusts internal SOPs can be found on QPulse.

1.5 This Code has been written to meet the requirements of the Information Governance regime which includes:-

1.5.1 The Data Protection Act 2018

1.5.2 The General Data Protection Regulation

1.5.3 Caldicott principles

1.5.4 The Human Rights Act 1998

1.5.5 The Computer Misuse Act 1990

1.5.6 The Copyright Designs and Patents Act

1.5.7 Freedom of Information Act 2000

1.5.8 The Bribery Act 2010

1.5.9 Confidentiality : NHS Code of Practice December 2014

1.5.10 Common Law Duty of Confidence

1.6 This Code has been produced to protect staff and patient data, by making them aware of the correct procedures in place so that they do not inadvertently breach any of these requirements. All staff are expected to meet the standards outlined in this document, much of which is built on existing good practice.

2 Definitions

2.1 **Data** – this is not defined under GDPR but the Regulation applies to the processing of personal data wholly or partly by automated means and to processing other than by automated means of data, which forms part of a filing system or which is intended to form part of a filing system. This can be in both written and electronic form

2.2 **Personal Data** –means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

2.3 **Special Categories of personal data**- this was previously known as "sensitive data". To process this category of data the Trust is required to comply with one of the conditions set out in Article 9 of the GDPR. This includes processing personal data about someone's:

- 2.3.1 Race and ethnicity
- 2.3.2 Political opinions
- 2.3.3 Religious or philosophical beliefs
- 2.3.4 Trade union membership
- 2.3.5 Processing of genetic data and biometric data for the purpose of identification
- 2.3.6 Health
- 2.3.7 Sex life
- 2.3.8 Sexual orientation

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

2.5 **Filing System** – means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3 (Duties) Roles & Responsibilities

3.1 The Chief Executive has overall responsibility for Data Protection within the Trust.

3.1.1 The implementation of and compliance with this policy is delegated to the Data Protection Officer (DPO) who is the Trust Secretary, Director of Corporate Compliance and Legal Services; Senior Information Risk Officer (SIRO) who is the Director of Finance and Business Services, the Information Governance Manager, Information Asset Owners (system Managers) and other designated personnel.

3.2 Management responsibilities:

The Medway NHS Foundation Trust will:

3.2.1 Ensure conditions for the fair collection and use of personal information is met by proactively informing patients and service users of how we collect, share, process, and protect their information (the confidentiality, integrity and availability of their information) and confirm to them the purpose for which their information will be used. This will mainly be done using the Trust's various privacy notices.

3.2.2 Collect and process only relevant and necessary personal information, to the extent that it is needed to fulfil operational needs or to comply with legal requirements.

3.2.3 Establish systems and processes to ensure that information is only kept for as long as lawfully required and in compliance with the Information Governance Alliance Records Management Code of Practice and the Trust Records Management Policies and SOP available via QPulse.

3.2.4 Ensure people whose information is held can fully exercise their rights under GDPR.

3.2.5 Take appropriate technical and organisational security measures to safeguard personal information whether using the existing Trust systems, or in transit to third parties.

3.2.6 Ensure personal information is not transferred outside the European Economic Area without suitable safeguards being evidenced via risk assessments and due diligence such as a Data Privacy Impact Assessment and a 'managing risks when outsourcing' document.

3.2.7 Ensure that there is a nominated person, the Data Protection Officer, with specific responsibility for data protection.

3.2.8 Ensure that there is a nominated person, the Caldicott Guardian, with specific responsibility for internal protocols governing access to the Trust's identifiable information.

3.2.9 Ensure that everyone managing and handling personal information is aware of their responsibilities.

3.2.10 Ensure that anyone who wants to make enquiries about handling personal information knows what to do and that clear procedures on handling personal information are in place.

3.2.11 Ensure that all staff who manage and handle personal information understand that they are contractually responsible for following good data protection practice.

3.2.12 Ensure that all staff who manage and handle personal information maintain awareness of their responsibilities and obligations to respect patient confidentiality.

3.2.13 Ensure that all staff who manage and handle personal information are appropriately trained to do so, and supervised where necessary.

3.2.14 Ensure that all staff who manage and handle personal information are aware that they are also personally liable if they breach legislation relating to gathering, storage or processing of data at all times.

3.2.15 Ensure that the performance of these procedures is regularly monitored and evaluated.

3.3 The Head of Corporate compliance, Risk and Information Governance holds management responsibility for

3.3.1 the processing of enquiries under GDPR,

3.3.2 The Information Governance Manager

3.3.3 Is responsible for advising users of their responsibilities under GDPR, Individual Rights (excluding the right of access)

3.3.4 Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.

3.3.5 Is responsible for liaising with external organisations on GDPR.

3.4 The Caldicott Guardian

3.4.1 Is responsible for agreeing, monitoring, and reviewing internal protocols governing access to personal-identifiable information by staff within the organisation, in compliance with UK and EU legislation and national and international policy and guidance.

3.4.2 Is responsible for agreeing, monitoring, and reviewing protocols governing the use of personal-identifiable information across organisations, e.g. with other NHS and local authority services, and other partner organisations contributing to the local provision of care.

3.5 Senior Information Risk Owner

3.5.1 Is responsible for the management and accountability of information risk.

3.5.2 All Staff are contractually and legally responsible for following good data protection practice and are liable if they breach legislation.

3.6 The Data Protection Officer:

3.6.1 Must ensure the Trust is GDPR compliant at all times and takes into consideration any new legislation that might take effect from time to time.

3.6.2 Has a responsibility to ensure requests under the GDPR, including Subject Access and the other Individual Rights are completed in a timely manner.

3.6.3 Is responsible for internal oversight of data security and protection breach investigations, and liaising with the ICO on serious breaches.

3.6.4 Is responsible for liaising with external organisations on GDPR.

3.6.5 Is responsible for ensuring the board is kept up to date on data protection legislation, guidance and requirements.

4 Principles

4.1 Confidentiality of Information

4.1.1 All employees are responsible for maintaining the confidentiality of information they become aware of during their employment by the organisation.

4.2 Definition of Confidential Information

4.2.1 Confidential or personal information can be anything that relates to patients, staff (including noncontract, volunteers, agency staff, locums, and student placements), their family or friends, however stored.

4.2.2 Personal information 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 photograph is sufficient to identify an individual. It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras as well as paper based systems.

4.2.3 Certain categories of information are legally defined as particularly sensitive and are protected by additional requirements stated in legislation (see definitions for full details).

4.2.4 To ensure the highest degree of protection of people's information, it is best to consider all information to be sensitive, even a patient's name and address.

4.3 Requests for Confidential Information

4.3.1 In line with the GDPR information can only lawfully be processed if:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;

- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

As part of its compliance with the GDPR, the Trust has taken steps to identify the ways in which information in relation to individuals is used by the Trust and a legal basis for each use of information. If you become aware of the Trust beginning to use or share data in a new way, you should bring this to the attention of the Data Protection Officer medwayft.dpo@nhs.net

4.4 Rights of the data subject

4.4.1 The GDPR provides the following rights for individuals; these are managed by the Data Protection Officer through the Information Governance Team and they are as follows:

- The right of access
- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.
- For more information please see the Individual's Rights SOP available via QPulse.
- All staff have a responsibility to ensure they know how to assist someone who wants to exercise one of these rights.
- Telephone Enquiries
- If a request for confidential information is made by telephone, always satisfy yourself as to the identity of the caller e.g.
- confirm the name, job title and department of the person requesting the information

- if in doubt, ask them to send you an email or call them back on their main switch board number.

4.5 Blagging

4.5.1 Some people attempt to gain information from organisations illegally by deception. This practice is known as “blagging”. An individual with a legitimate request will be open about their activity and will not need to resort to blagging. You should not disclose any information unless you are sure they are the person they say they are and you are confident that the reasons they have provided means they will need access to the information as part of their job role. If in any doubt, do not disclose the information but speak to your manager or contact the Information Governance Team.

4.6 Cyber Security

4.6.1 All staff must be aware of Cyber Security and know what to do if you believe the Trust has been subject to an attack. Common forms of attack are:

4.6.2 Junk – Junk email (also known as spam) is unwanted or unsolicited advertising or promotional material.

4.6.3 Malware – A term used to refer to various forms of intrusive or hostile computer software, such as viruses, worms and trojan horses.

4.6.4 Phishing – The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

4.6.5 Spam – Irrelevant or unsolicited messages sent over the Internet, typically to a large numbers of users, for the purposes of advertising, phishing, spreading malware etc.

4.6.6 Spoofing – The creation of email messages with a forged sender address. A forged sender address uses a respected or reputable origin email address to conceal the fact that the email has come from elsewhere.

4.6.7 If you receive an email from a familiar organisation or contact which you believe to be suspicious, such as an unusual request to access patient data or a payment request:

4.6.8 Do not open attachments or follow links

4.6.9 Validate the request by contacting the organisation or person through normal established channels (e.g. make a call to a verifiable telephone number or manually navigate to the organisation’s website)

4.6.10 Report all suspected spam to the IT service desk for analysis and blocking.

4.7 Requests for Confidential Information by the Police

4.7.1 The Trust has a SOP on dealing with Police requests. This can be found on QPulse

4.7.2 Don’t be bullied into giving out confidential information. If in doubt, check with a senior member of staff or the Information Governance team.

4.8 Requests for Confidential Information by the media

4.8.1 Should you receive Media requests please direct them to the Communications team on: communications.medwayft@nhs.net or 01634 833962.

4.9 Abuse of Privilege

4.9.1 All NHS staff are strictly forbidden to access their own personal information unless specifically authorised to do so. Any staff wishing to access their own information should make a request through the same channels as a member of the public. In addition, staff are forbidden to access any personal information relating to public figures, colleagues, friends or relatives unless they have a legitimate reason to do so as part of their employment responsibilities. All systems used in the Trust have electronic audit trails which are monitored regularly by the Information Governance team and by Information Asset Owners. Staff found to have deliberately accessed records without a legitimate business reason will be reported to HR for disciplinary investigation. If the individual is found to be guilty, the case will be reported to the Information Commissioners Office and the police. The consequences can include:

- Fines of up to £5,000 in a Magistrates' Court
- Unlimited fines if the case goes to the Crown Court
- Prison sentences for serious breaches
- Profession accreditation being revoked
- A criminal record

4.10 Carelessness

4.10.1 do not talk about patients or staff in public places or where you can be overheard

4.10.2 do not leave any medical or staff records or confidential information lying around unattended

4.10.3 make sure that any computer screens, or other displays of confidential information i.e. whiteboards, cannot be seen by anyone who does not need to know.

4.11 Transfer of information including fax, email and taking information home.

4.11.1 All staff must ensure that the information is sent in line with the Trusts Transfer of Information Policy which is available via Qpulse.

4.12 Management of records including destruction.

4.12.1 All staff must ensure that records are kept and disposed of in line with the Overarching Records Management Policy which is available via Qpulse. This policy also includes guidance on the destruction of information in both electronic and hard copy format.

4.13 Confidentiality of passwords and user names

4.13.1 Passwords and usernames should never be shared or written down in note books or diaries.

4.13.2 They should never be shared with team members.

4.13.3 No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges of other employees. Any attempts to breach security should be immediately reported to the IT Help Desk or Information Governance Team and may result in disciplinary action being taken as a result of the associated possible breach of the Computer Misuse Act 1990 and/or the GDPR . All breaches of IT security or confidentiality must be reported through the Trust's incident reporting system (Datix).

4.14 Electronic devices, USB, laptopss, phones

4.14.1 Only Trust provided electronic devices (included but not limited to USB, laps, mobile phones) should be used when handling identifiable information

4.14.2 It is acceptable to use NHS.net on personal devices however no attachments should be saved on personal devices

4.15 General Provisions for Audits

4.15.1 Confidentiality Audits are carried out each year on site and will seek to identify non-compliance with the Code and associated policies. Audit results will be reported to the Information Governance team to assess the need for further training or development of the Code.

4.16 Interpretation

4.16.1 If a member of staff has any questions about the Code they should discuss this with their manager or the Information Governance team met-tr.InformationGovernanceMedFT@nhs.net

4.17 Non-Compliance

4.17.1 Non-compliance with this Confidentiality Code of Conduct by any person working for the organisation is regarded as a serious offence (gross misconduct) and could lead to summary dismissal even as a first offence.

4.18 Resignation

4.18.1 Staff must ensure that on their last day they hand in to their line manager, their name badge and any mobile/electronic devices issued to them. They must also ensure that hand overs are completed and NHSmail inboxes have all Trust emails deleted.

4.19 Incident reporting

4.19.1 All staff must ensure that incidents relating to breaches of data security and awareness are reported through the Datix system. Full details of reporting an information governance incident can be found on QPulse

5 Monitoring and Review

What will be monitored	How/Method/ Frequency	Lead	Reporting to	Deficiencies/ gaps Recommendations and actions
Policy review	First review in one year and then every year years	Information Governance Manager	Data Protection Officer	

6 Training and Implementation

6.1 All staff must complete their annual Data Security and Awareness Training either on-line or via a classroom based session. Full details can be found https://intranet.medway.nhs.uk/directorates-and-departments/corporate-governance-risk-compliance-legal/information-governance/data-security-awareness-training/

7 Equality Impact Assessment Statement & Tool

All public bodies have a statutory duty under The Equality Act 2010 (Statutory Duties) Regulations 2011 to provide "evidence of analysis it undertook to establish whether its policies and practices would further, or had furthered, the aims set out in section 149(1) of the [Equality Act 2010]"; in effect to undertake equality impact assessments on all procedural documents and practices. Authors should use the Equality Impact Toolkit to assess the impact of the document.
In the first instance this will mean screening the document and, where the screening indicates, completing a full assessment. The Toolkit can be found on the Trust website http://www.medway.nhs.uk/our-foundation-trust/publications/equality-and-diversity/equality-impact-assessments/

A document will not be considered approved until the author has confirmed that the screening process has been carried out and where required a full impact assessment has been completed. Where a full assessment is completed this should be submitted along with the document for approval.

8 References

Document	Ref No
References:	
NHS Digital guidance	
Information Commissioners Office	
The Data Protection Act 2018	
The General Data Protection Regulation	
Caldicott principles	

Code of Conduct for Employees in Respect of Confidentiality

The Human Rights Act 1998	
The Computer Misuse Act 1990	
The Copyright Designs and Patents Act	
Freedom of Information Act 2000	
The Bribery Act 2010	
Confidentiality : NHS Code of Practice December 2014	
Common Law Duty of Confidence	
Trust Associated Documents:	
POLCGR077 - Secure Transfer of Information Policy (Was Safe Haven Policy)	POLCGR077
POLCGR007 - Data Protection Policy	POLCGR007
POLCGR018 - Information Security Policy	POLCGR018
POLCGR113 - Acceptable Use of Trust Information Systems and Asset Policy	POLCGR113

END OF DOCUMENT