Kent Community Health
NHS Foundation Trust

STAFF CONFIDENTIALITY CODE OF CONDUCT

For all staff, including Employees, Bank, Locum, Agency Workers, Contractors, Volunteers and any other person working for, or on behalf of Kent Community Health NHS Foundation Trust

This Code outlines your responsibilities in protecting the personal data you come into contact with during your employment with Kent Community Health NHS Foundation Trust and the Trusts' expectations of your conduct.

It has been produced to ensure you are aware of your legal responsibility to preserve confidentiality and is issued to all employees at the start of their employment with the Trust.

Personal data means any information (paper, electronic, audio/tape, video, verbal, etc.) from which an individual can be identified either 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 their physical, physiological, genetic, mental, economic, cultural or social identity. It also relates to sensitive personal information including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic / biometric data, health, data concerning sex life or sexual orientation.

This Code applies to the data of both living and deceased individuals.

Know Your Obligations
All individuals working on behalf of the trust have a duty of confidentiality regarding personal information. This is based on the Data Protection Act 2018, UK General Data Protection Regulations and other laws, decisions made about the law in Courts, employment contracts, organisational policy and professional regulatory obligations and codes of conduct for most registered health or other practitioners. Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution as well as opening the Trust to legal claims and the potential of significant fines.

Therefore, you must not:

- Put personal information at risk of unauthorised access.
- Misuse any personal information or allow others to do so.
- Access information, including your own, without a legitimate reason to do so as part of your job, or the direct care of the patient.
- Ensure you remain aware of current Information Governance Policies and Procedures which can be found on flo.

Keep Personal Information Private
You must comply with the rules laid out in the Trust's Information Governance and Cyber Security Policies and guidance, all of which are available in full on Flo. These policies and guidance documents give practical advice to keep personal data protected.

Disclose with Appropriate Care
The Trust will ensure that patients and staff are adequately informed about the use and disclosure of their personal information by the use of Staff and Patient Privacy Notices and posters which will tell them how and why their personal information is used. You must ensure you are familiar with this patient information material and seek advice from the Information Governance Team if you are asked questions that you are unable to answer.

If you are authorised to disclose personal information you must only:

- Share with those with a legitimate right to see/hear the information.
- Transfer information in line with the Trust's secure transfer methods.
- Disclose the minimum necessary to provide safe care.

Please see the 'Share Information for Direct Care' flowchart.

Under Common Law, identifiable information may be disclosed without consent when:

- There is a legal duty to do so, for example a Court Order;
- It is necessary to safeguard the individual, or others, or is in the public interest, such as where the public good outweighs obligation of confidentiality to the individual concerned.

During office hours, refer all requests for disclosure of personal information without the consent of the individual, including requests from the police, to the Legal Services Team.

Out of hours these must be referred to the Service Manager or on call director. All decisions to disclose must be fully documented.

Kent Community Health
NHS Foundation Trust

Senior IG Roles

SIRO

A Senior Information Risk Owner (SIRO) is an Executive Director or member of the Senior Management Board of an organisation with overall responsibility for organisational information risk within policy. The SIRO is accountable and responsible for information risk across the organisation.

Name: Gordon Flack

Main role:
Chief Finance Officer

Email:
gordon.flack@nhs.net

Contact number:
Office/Mobile 07432 739422

Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.

Name: Dr Sarah Phillips

Main role:
Chief Medical Officer

Email:
kcht.caldicottguardian@nhs.net / sarahphillips4@nhs.net

Contact numbers:
Office - 01622 211922 or Mobile 07391 861077

Data Protection Officer

The primary role of the DPO is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Name: Mark Gray

Main role:
Director of ICT

Email:
kentchft.dataprotectionofficer@nhs.net

Contact number:
Office 0300 123 2079

Kent Community Health
NHS Foundation Trust

INFORMATION GOVERNANCE AND CYBER SECURITY DOCUMENTS

Please ensure you are familiar with the contents of the Trust's policies and guidance below, sign and date to say you have read and understood these policies. If you require any assistance, do not understand any aspect, or wish to have access to an accessibility version such as large print, please contact your manager.

DOCUMENT TITLE	SIGN	DATE
Data Security and Protection Policy		
Cyber Network and Information Systems Policy		
Audio-Visual Recording Protocol		
Home Remote and Mobile Working		
Access to Records Policy		
Freedom of Information Act 2000 Policy		
Secondary Use of Patient Personal Data Policy		
Video Conferencing and Consultations		
Use of Email		
IT Evidence Seizure		
Instant Messaging		
Flo App		
Data Quality Policy		
Rio SOP		
Audio Visual Recording Protocol		
IG Linkworkers Support Pack (if required for your role)		
IG Essentials Workspace		

HOW TO GUIDES		
Texting, emailing, voicemail guidance for staff		
Clear screen and clear desk procedure		
Emails - how to use and store		
How to archive flowchart		
How to ensure the security and confidentiality of records		
How to keep a clinical diary and printed caseload tool		
How to lock printing_Not papercut		
How to obtain and use the NHS number		
How to scan records		
How to send confidential information through the post		
How to share information with the police		
How to share information Caldicott principles		
How to transport paper clinical and staff records		
Move management process		
Risk assessment for transportation and storage of confidential information offsite		
How to determine if your Service is a data controller or a processor		
How to share information for direct care flowchart		

Manager checklist for information governance		
Safe haven guidance: including transport, post, telephone, email, printing		
Send secure emails to unencrypted emails		
Email or text patients (Accessible information standard)		
Archiving - How to review, retain and dispose of records		
Checklist for information held at a non-KCHFT site		
Manager checklist for investigating IG incidents		
FOI (Freedom of Information)		

I, _____, confirm that I have read and understood all documents listed above and will work within all Trust policies, procedures and processes including those set out within my contract of employment.

Signature: _____ Date: _____

Key Contacts

IG Team

If your enquiry is routine please contact via TopDesk > Corporate Operations > Information Governance.

If your enquiry is of an urgent nature, i.e. regarding an incident, please call the team on 0300123 2079

Cyber Security

Please contact Cyber Security Specialist either via the IT Helpdek on TopDesk or phone 0300 123 1885.

FOI Team

Please email kcht.foi@nhs.net.

Estates Team

For move management issues or confidential waste enquiries -

0300 303 3186 or kentchft.estateshelpdesk@nhs.net