South Eastern Health and Social Care Trust

Policy Code: SET/Gen (09) 2020

SOUTH EASTERN TRUST

Title:	**Code of Practice on Protecting the Confidentiality of Service User Information**			
Author(s)	**Head of Information Governance & Directorate Support**			
Ownership:	**South Eastern health & Social Care Trust**			
Approval by:	**Information Governance Steering Committee**		**Approval date:**	**October 2020**
Operational Date:	**October 2020**		**Next Review:**	**October 2023**
Version No.	**3.2**	**Supercedes**	**SET/Gen (145) 2016**	
Key Word	**Confidentiality**			
Links to other policies	**Department of Health** **Code of Practice on Protecting the Confidentiality of Service User Information – DHSSPS – April 2019** **Privacy Advisory Committee**			

1.0 INTRODUCTION

1.1 Background

1.1.1 The use and sharing of service user personal information forms an essential part of the provision of Health & Social Care (HSC). It benefits individual service users, enables health & social care to function effectively and is often necessary in the public interest. The Department of Health (Formerly the Department of Health Social Services & Public Safety [DHSSPS]) Code of Practice on Confidentiality, April 2019, provides support and guidance for all those involved in Health & Social care, concerning decisions about the protection, use and disclosure of service user information.

1.1.2 The Code has been developed by the Privacy Advisory Committee, following a comprehensive round of public consultation during 2011. The Code was subject to review in 2018/2019 by the Department of Health (DoH) and updated to take account of the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

1.1.3 The Trust regards the lawful and correct handling of personal data by staff of the South Eastern HSC Trust (the Trust) as crucial to successful operations and to maintaining confidence between ourselves and our internal and external clientele.

1.2 Purpose

1.2.1 The Code of Practice is a specific part of the Trust's overall corporate programme and related to other policies, such as:-

- The Data Protection Policy
- Records Management Policy and Procedure
- Freedom of Information Policy and Procedure
- Email Policy

1.2.2 The purpose and aim of this policy is to:-

- Provide a framework for the legal, secure and confidential management of information; and
- Ensure optimum protection for patients, services users and staff in compliance with current legislation.

(Please refer to the Information Governance (IG) i-connect site for a copy of all IG Policies and Procedures.)

2.0 SCOPE OF THE POLICY

2.1 This policy applies to all staff throughout the Trust.

2.2 The Code of Practice provides a best practice resource for health and social care workers of all grades and professional groups and is available for use in all health and care settings including, hospital, community, primary care and the private and voluntary sectors.

3.0 ROLES/RESPONSIBILITIES

3.1 **Chief Executive**: The Chief Executive as the Accountable Officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to protect the confidentiality of service user information. The Chief Executive Officer has a particular responsibility for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

3.2 **Director of Human Resources & Corporate Affairs**: is the lead Director/Senior Information Risk Owner (SIRO) for the Trust. The Director of Planning, Information and Performance Management has been appointed Deputy SIRO.

This Director in conjunction with all other Directors, Assistant Directors/Information Asset Owners and Senior Managers is responsible for the implementation of the Code of Practice. Responsibilities also include:-

- Promotion and overseeing of an Information Governance agenda (includes Data Protection, Confidentiality and Records Management).
- Ensuring that the Information Governance function is supported in terms of commitment and resources.
- Reporting to Trust Board on the on-going operation of Information Governance issues and,

- Ensuring that Information Governance is considered in the planning process and in the setting and monitoring of budgets.

3.3 **Personal Data Guardians**: The Trust's Data Guardians (Medical Director and the Director of Children's Services & Executive Director of Social Work) have a particular responsibility for reflecting service user's interests regarding the use of service user identifiable information. They are responsible for ensuring patient/client identifiable information is shared in an appropriate and secure manner.

3.4 **Assistant Director, Risk Management & Governance**: is accountable to and reports to the Director of Human Resources and Corporate Affairs and is the nominated operational Assistant Director for the delivery of the strategic and operational management agenda for Information Governance.

3.5 **Head of Information Governance & Directorate Support/ Data Protection Officer**: is accountable to the Assistant Director, Risk Management & Governance. His/her role is to support the Trust in the development, implementation and review of Information Governance strategy, policies and procedures (local and regional).

3.6 **Directors**: Each Director is accountable for the management of risks within their own areas of specific responsibility. They are responsible for ensuring that effective arrangements for protecting service user information are in place across all services for which they are responsible. The arrangements should be in line with the guidance detailed within the Code of Practice and should integrate with existing management and professional arrangements and processes.

3.7 **Assistant Directors/Information Asset Owners (IAO)**: Each IAO is responsible for the processing of data within their Directorate and as such must maintain and review on an annual basis an information asset register for their Directorate. The IAO is also responsible for the management of information governance risk. This is incorporated into their quarterly directorate risk review and annual risk register submission to the Risk Committee.

3.8 **Information Asset Assistants (IAA):** IAA's are (4th line managers / Governance Facilitators or IAO's nominated senior manager). These individuals are familiar with the business functions and data processing within their Directorate and for ensuring that staff are compliant with professional standards, Trust policy and procedure in respect of all aspects of IG.

3.9 **Information Governance Sub Committee (IGSC)**: The Trust's Information Governance Sub Committee is responsible for ensuring that this Policy is implemented and adherence monitored, through for example, collection of incident data. The IGSC reports to the Corporate Control Committee, which reports to the Governance Committee.

3.10 **Local Records Managers**: The responsibility for local adherence to this Policy is devolved to the relevant Directors, Assistant Directors/IAOs, Senior Managers and Department Managers. All Heads of business functions and other units within the Trust have overall responsibility for the protection of

service user information in a way which meets the aims of Trust Policy and the Code of Practice.

3.11 All staff: It is the responsibility of all staff to familiarise themselves and adhere to the contents of this Policy Statement and the DHSSPS Code of Practice on Protecting the Confidentiality of service user information.

4.0 KEY POLICY PRINCIPLES

4.1 Policy Principles

The Code of Practice is principally concerned with identifiable service user information. Uses or disclosures of such information are only justified where either:-

- Service user consent has been given, or
- There is a statutory requirement, or
- The balance of public and private interest favours disclosure.

The Code of Practice standardises the practice of protecting the confidentiality of service user information across Northern Ireland.

5.0 IMPLEMENTATION OF POLICY

The confidentiality of service user information must always be of primary concern to Trust staff. All staff who process service user information will receive the necessary training and formally acknowledge their duty of care with regard to confidentiality of service user information.

5.1 Dissemination

This policy will be made available to all staff via the intranet and via their line manager.

5.2 Resources/Training

5.2.1 All Trust staff will be made aware of their responsibilities for protecting the confidentiality of service user information through generic and specific training programmes and guidance. An 'employees guide to handling information' booklet is available via the intranet and hard copy on request from the IG department.

5.3 Exceptions

This procedure applies to all areas of the Trust. There are no exceptions.

6.0 MONITORING

6.1 The Trust will follow the guidance provided in the Code of Practice within all relevant procedures and guidance used for operational activities.

Interpretation of the Code of Practice will be monitored via the Information Governance Steering Committee.

6.2 Wilful breach of this policy can result in disciplinary action in line with the Trust's Disciplinary Policy. The Legislative framework appropriate to this area i.e. the Data Protection and Freedom of Information Acts, means that there is a possibility of legal action being taken against the Trust and/or individuals involved if/?in the event of a confidentiality breach.

7.0 EVIDENCE BASE/REFERENCES

Data Protection Act (2018)
https://ico.org.uk/for-organisations/guide-to-data-protection/

The General Data Protection Regulation (EU) 2016/679 (GDPR)
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information, 2019 Available at
http://iconnect/HRCorporateAffairs/RiskManagementGovernance/InformationGovernance/IG%20Policies%20and%20Procedures/Code%20of%20Practice%20on%20Protecting%20Confidentiality%20of%20Service%20User%20Information%20DOH%20April%202019.pdf

Freedom of Information Act (2000)
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

South Eastern HSC Trust Information Governance iconnect
http://iconnect/HRCorporateAffairs/RiskManagementGovernance/InformationGovernance/Pages/default.aspx

If staff require further guidance on this matter they may be directed to the Information Governance Department, Lough House, Ards Community Hospital site. Alternatively staff may wish to visit the Information Governance intranet site and our FAQs which is available at:-

http://iconnect/HRCorporateAffairs/RiskManagementGovernance/InformationGovernance/Pages/default.aspx

8.0 CONSULTATION PROCESS

The revision of this Policy has been consulted via the Information Governance Steering Committee to reflect the changes in the DHSSPS Code of Practice on Protecting the Confidentiality of Service User Information. Publication of the revised Policy was approved on 30 June 2020.

9.0 APPENDICES/ATTACHMENTS

There are no appendices/attachments.

10.0 EQUALITY STATEMENT

In line with duties under the equality legislation (Section 75 of the Northern Ireland Act 1998), Targeting Social Need Initiative, Disability discrimination and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.
The outcome of the Equality screening for this policy is:

Major impact ☐

Minor impact ☐

No impact. ✓

SIGNATORIES

(Policy – Guidance should be signed off by the author of the policy and the identified responsible director).

Policy Name	Author Endorsement	Modified	Modified By
Code of Practice on Protecting the Confidentiality of Service User Information	Yes	15/10/2020 05:03 PM	McAree, Lynda

Policy Name	Approval	Modified	Modified By
Code of Practice on Protecting the Confidentiality of Service User Information	Endorsed	11/11/2020 04:32 PM	Martyn, Charlie