South Eastern Health and Social Care Trust

Policy Code: SET/Gen (146) 2016

SOUTH EASTERN TRUST

Title:	**Data Protection Policy Statement**			
Author(s)	**Head of Information Governance & Directorate Support**			
Ownership:	**South Eastern Trust**			
Approval by:	**Information Governance Steering Committee**		**Approval date:**	**September 2015**
Operational Date:	**August 2016**		**Next Review:**	**August 2018**
Version No.	**3.0**	**Supercedes**	**SET/Gen (60) 2012**	
Key word/s	**Data Protection**			
Links to other policies	**Evidence Base: References at end of policy** **ISO Office Procedures for Processing Subject Access Requests**			

1.0 INTRODUCTION/PURPOSE OF POLICY

1.1 Background

1.1.1 The South Eastern HSC Trust (hereafter referred to as the Trust) needs to collect, use and process personal data, including *sensitive data,* about the people with whom it deals. These people include current, past and prospective patients, clients, staff, service providers and suppliers. In addition the Trust is required by law to collect and use certain types of information to comply with requirements of government departments for example medical records, social service data, public health data, statistics, business data etc. This information must be managed within a framework which provides optimum protection for patients, clients, staff & customers alike – i.e. in compliance with current legislation, the Data Protection Act 1998, and extending beyond this to take account of Caldicott recommendations and the general duty of confidentiality.

1.1.2 The Trust regards the lawful and correct handling of personal data by the staff of the Trust as crucial to successful operations and to maintaining confidence between ourselves and our internal and external clientele.

1.1.3 The Data Protection policy is a specific part of the Trust's overall corporate programme and related to other policies, such as:-

- Information Governance Strategy
- Records Management Policy
- Freedom of Information
- Information Communication & Technology (ICT) Strategy

1.1.4 In addition, the Trust adheres to and has implemented the following Department of Health Social Services & Public Safety (DHSSPS) and Health & Social Care (HSC) Guidelines and Protocols:-

- Protocol for Sharing Service User Information for Secondary Purposes 2011
- Good Management: Good Records, December 2011 (under revision)
- Code of Practice on Protecting the Confidentiality of Service User Information, January 2012

1.2 Purpose

The purpose and aim of this policy is to:-

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

2.0 SCOPE OF THE POLICY

This policy applies to all Trust employees and to Non-Executive Directors.

3.0 ROLES/RESPONSIBILITIES

3.1 All Trust employees including Non-Executive Directors have responsibilities under data protection. The Trust has identified the data guardians (the Medical Director and the Director of Children's Services & Executive Director of Social Work) as the individuals within the Trust with specific responsibility for data protection. In addition, and in line with DHSSPS Information Governance Framework, the Trust has also appointed Senior Information Risk Owners and Information Asset Owners (IAO). The SIRO role is undertaken by the Director of Human Resources and Corporate Affairs. The Director of Planning, Information & Performance Management has been appointed Deputy SIRO. All Assistant Directors undertake the role of the Information Asset Owner in relation to all information processed within their Directorate.

3.2 The Trust also ensures that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice, is trained to do so, and appropriately supervised. Staff managing and handling personal information must also ensure that queries about personal data are dealt with promptly and courteously in accordance with guidelines.

4.0 KEY POLICY PRINCIPLES

4.1 The main focus of this policy statement is on providing guidance in relation to the protection, sharing and disclosure of patient/client/staff information, but it

is important to stress that maintaining confidentiality and adhering to data protection legislation applies to all Trust staff.

4.2 To this end, the Trust fully endorses and abides by the principles of data protection. Specifically, the principles require that:-

1. *Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;*
2. *Personal information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*
3. *Personal information shall be adequate, relevant and not excessive in relation to the purpose for which they are processed;*
4. *Personal information shall be accurate and where necessary, kept up to date;*
5. *Personal information should not be kept for longer than is necessary for that purpose or those purposes;*
6. *Personal information shall be processed in accordance with the rights of data subjects under the Act;*
7. *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;*
8. *Personal information shall not be transferred to a country or territory outside the European Economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

4.3 The Trust will through appropriate management, strict application of criteria, guidelines and directives :-

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held, are able to be exercised under the Act subject to limitations as laid down in the legislation. (These include the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information);
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that all staff are adequately trained for their roles and responsibilities.

4.4 Wilful breach of this Policy can result in disciplinary action in line with the Trust's Disciplinary Policy. The legislative framework relating to records management, especially 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.

5.0 IMPLEMENTATION OF PROCECURE

5.1 Dissemination

This policy will be made available to all staff via the intranet.

5.2 Resources

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. Data Protection training is available online.

5.2.2 As part of staffs' Personal Development Contribution Review (PDCR) Managers should ensure that Information and Knowledge dimensions (IK1, IK2 & IK3) are included.

5.3 Exceptions

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

6.0 MONITORING

This procedure will be reviewed every 3 years (or sooner if new legislation, codes of practice or national standards are introduced).

7.0 REFERENCES

The Data Protection Act, 1998 available at :-
http://www.legislation.gov.uk/ukpga/1998/29/contents
DHSSPS *Good Management: Good Records, December* 2011 DHSSPS available at:-
http://www.dhsspsni.gov.uk/gmgr.htm
DHSSPS & HSC *Protocol for Sharing Service User Information for Secondary Purposes* available at:-
http://setintranet/filestore/publications/dhssps___hsc_protocol_for_sharing_service_user_information_for_secondary_purposes__final__pdf_.pdf
DHSSPS *Code of Practice for Protecting the Confidentiality of Service User Information*, 2012 available at:-
http://setintranet/filestore/publications/Code_of_Pratice_on_Protecting_the_Confidentiality_of_Service_User_Information.pdf
Information Governance i-connect site
http://setintranet/departments/information_governance/

8.0 CONSULTANTION PROCESS

The revision of this Policy has been consulted via the Information Governance Steering Committee and Senior Managers within the Risk Management & Governance Directorate.

9.0 APPENDICES / ATTACHMENTS

NA

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).

Form Status	Policy Name	Type	Author Endorsement	Modified By
Directorate	Data Protection Policy Statement		Yes	McAree, Lynda

Form Status	Policy Name	Approval	Modified	Modified By
Read Only	Data Protection Policy Statement	Endorsed	26/08/2016 12:34 PM	Weir, Myra