**Policy Checklist**

<table>
<thead>
<tr>
<th>Name of Policy:</th>
<th>Information Technology Transfer of Electronic Data Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose of Policy:</td>
<td>To update the previous Information Technology Transfer of Electronic Data Policy dated 12 December 2011, version number 3.1. The purpose of the Policy is to provide guidance for those staff who need to transfer electronic data securely. To ensure staff within the Trust who need to legitimately use USB pens, CDs, laptops and floppy disks etc to transfer data between facilities in the course of their work, can do so safely. The updated policy also reinforces staff responsibility in relation to storage of corporate Data on non-Trust devices e.g. a home computer. The policy also ensures that the Trust has robust security mechanisms in place to deal with all removable media and staff are aware of the need to use adequate data encryption measures. The policy also outlines the roles and responsibilities for staff when transferring electronic data.</td>
</tr>
<tr>
<td>Directorate responsible for Policy</td>
<td>Directorate of Performance and Reform</td>
</tr>
<tr>
<td>Name &amp; Title of Author:</td>
<td>Stephen Hylands, Head of Information Technology</td>
</tr>
<tr>
<td>Does this meet criteria of a Policy?</td>
<td>Yes</td>
</tr>
<tr>
<td>Trade Union consultation?</td>
<td>Yes</td>
</tr>
<tr>
<td>Equality Screened by:</td>
<td>Stephen Hylands, Head of Information Technology</td>
</tr>
<tr>
<td>Date Policy submitted to Policy Scrutiny Committee:</td>
<td>16th December 2013</td>
</tr>
<tr>
<td>Members of Policy Scrutiny Committee in Attendance:</td>
<td>Vivienne Toal, Head of Employee Engagement &amp; Relations (Chair), Melanie McClements, Assistant Director of Older People’s Services, Claire Graham, Head of Corporate Records (for Siobhan Hanna), Marita Magennis, Head of Social Work and Social Care Governance, Fiona Wright, Assistant Director of Nursing Governance, Daphne Johnston, Clinical &amp; Social Care Governance Manager</td>
</tr>
<tr>
<td>Policy Approved/Rejected/Amended</td>
<td>Approved</td>
</tr>
<tr>
<td>Policy Implementation Plan included?</td>
<td>Yes</td>
</tr>
<tr>
<td>Any other comments:</td>
<td></td>
</tr>
<tr>
<td>Date presented to SMT</td>
<td></td>
</tr>
<tr>
<td>Director Responsible</td>
<td>Mrs Paula Clarke</td>
</tr>
<tr>
<td>SMT Approved/Rejected/Amended</td>
<td></td>
</tr>
<tr>
<td>SMT Comments</td>
<td></td>
</tr>
<tr>
<td>Date received by Employee Engagement &amp; Relations for database/Intranet/Internet</td>
<td>16 December 2013</td>
</tr>
<tr>
<td>Date for further review</td>
<td>2 year default</td>
</tr>
</tbody>
</table>
### POLICY DOCUMENT – VERSION CONTROL SHEET

| **Title** | Title: Information Technology Transfer of Electronic Data Policy  
Version: 3.2  
Reference number/document name: |
|-----------|------------------------------------------------------------------------|
| **Supersedes** | Supersedes: Information Technology Transfer of Electronic Data Policy version: 3.1  
Description of Amendments(s)/Previous Policy or Version:  
Update to Information Technology Transfer of Electronic Data Policy version: 3.1 detailing staff responsibilities when storing corporate data on non-Trust devices. |
| **Originator** | Name of Author: Stephen Hylands  
Title: Head of Information Technology |
| **Scrutiny Committee & SMT approval** | Referred for approval by:  
Date of Referral:  
Scrutiny Policy Committee (Date)  
SMT approval (Date) |
| **Circulation** | Issue Date:  
Circulated By:  
Issued To: As per circulation List (details below) |
| **Review** | Review Date: October 2013  
Responsibility of (Name): Stephen Hylands  
Title: Head of Information Technology |
Southern Health and Social Care Trust Transfer of Electronic Data Policy

POLICY FOR THE TRANSFER OF ELECTRONIC DATA

Stephen Hylands
1.0 Introduction

1.1 The Southern Health & Social Care Trust (hereafter referred to as the “Trust”) Transfer of Electronic Data Policy is based on NHS Information Governance guidelines and policies.

1.2 Following on-going data security breaches across the Her Majesty’s Revenue & Customs, the DVLA and various NHS Trusts over the last few years, Data Loss Prevention is recognized as a critical priority for the Trust. In May 2012, a fine of £325,000 was imposed by the Information Commissioners Office on Brighton and Sussex University Hospitals after patient information was found on employee owned computers, which employees had sold. More recently in July 2013 The Information Commissioners Office issued NHS Surrey with a fine of £200,000 after more than 3,000 patient records were found on second hand computers bought through an online auction site.

1.3 Turning a blind eye to the presence of insecure removable media in the workplace not only leads to data protection breaches, but can lead to public relations disasters and a loss of confidence among the public. It is vital that the Trust provides guidance for staff on removable media when transferring information.

1.4 Any patient data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop or USB pen must be encrypted (only Trust approved encrypted USB pens should be used for storing patient identifiable information). This is a requirement across all public sector organisations set by the Cabinet Secretary.

1.5 Every effort must be made to ensure that the transfer of confidential (patient identifiable) electronic information is secure. Methods of transfer include removable media, email and laptop.

1.6 This policy should be read in conjunction with:

- ICT Security Policy
- Email Policy
- Encryption of Emails (Guidance)

1.7 In accordance with the Data Protection Act 1998 every person working for, on behalf of, or within the Trust must ensure that confidential information is only made available to those who are authorised to receive it.

1.8 This policy has been developed in accordance with the Trusts key principles for policy development.

1.9 This policy has been developed in consultation with the appropriate internal stakeholders.
2.0 Purpose and Aims

2.1 The purpose and aim of this policy is to:

2.1.1 Provide guidance for those staff who need to transfer electronic data securely;

2.1.2 ensure staff within the Trust who need to legitimately use USB pens, CDs, laptops and floppy disks etc to transfer data between facilities in the course of their work, can do so safely;

2.1.3 ensure that the Trust has robust security mechanisms in place to deal with all removable media;

2.1.4 ensure that the Trust staff are aware of the need to use adequate data encryption measures;

2.1.5 ensure that staff have clear understanding of their roles and responsibilities when transferring electronic data.

2.1.6 ensure staff are fully aware of their responsibilities in relation to storage and disposal of Trust data on non-Trust devices such as a home computer.

3.0 Policy Statement

3.1 This policy has been developed to prevent unauthorised disclosure, modification, storage, removal or destruction of Trust electronic information, which could cause disruption to Trust business activities.

For the purpose of this policy, transferable media is defined as electronic data. This policy is applicable to all electronic data which is confidential or patient identifiable.

4.0 Scope of the Policy

4.1 This policy is applicable to all staff who use removable media owned or operated by the Trust. Removable media include tapes, Floppy discs, removable or external hard disc drives, optical discs DVD and CD-rom, solid state memory devices including memory cards and USB sticks / pen drives etc

4.2 This policy is applicable to all staff who need to transfer confidential or patient identifiable data electronically. Only E-gif approved encryption algorithms should be used to encrypt and protect relevant Trust data i.e. 3DES, AES or Blowfish and should be used at a recommended 256bit
strength. Such software or encrypted UBS pens will be made available to relevant staff on request.

4.3 This policy applies to all staff who wish to send confidential information through courier services.

4.4 The policy also applies to staff who use a Trust encrypted memory stick.

5.0 Responsibilities

5.1 The Trust Chief Executive, as ‘Accountable Officer’ has overall responsibility for ensuring the aims of this policy are met; the Director of Performance & Reform (Executive Director with responsibility for ICT) has delegated responsibility.

5.2 Role of Front-Line Staff

5.2.1 Staff and contractors are not permitted to introduce or use any removable media other than those provided or explicitly approved for use by the Trust. Staff who have been authorised to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as required by this policy. Staff involved in data extraction and data file creation must receive appropriate Information Governance training.

5.2.2 Where staff need to use removable media to transfer patient identifiable data or confidential information, they must use encryption software or encrypted USB pens supplied only by IT.

5.2.3 All staff have responsibility for maintaining the security and confidentiality of personal / sensitive information. This includes information that may be stored on non-trust devices e.g. home computers is appropriately disposed of when no longer required.

5.3 Role Of Line Managers

5.3.1 Line managers in collaboration with the IT Department are responsible for the day to day management and oversight of removable media used within their work areas to ensure this policy is followed.

5.3.2 Line managers are responsible for the secure storage of all unallocated removable media and its related control documentation as required by this procedure.

5.3.3 Line managers are responsible for educating staff on the appropriateness of data encryption software in relation to confidential data and sending email attachments via the internet. The IT Department will assist Line Managers with this, if required.
5.3.4 Line Managers should ensure that all staff are aware of their responsibilities regarding data stored on home computers.

5.4 Role of the Head of IT

5.4.1 The Head of IT is responsible for ensuring that the Southern HSC Trust has appropriate data encryption capabilities in order to protect data that is processed on removable media.

5.4.2 The Head of IT is responsible for assuring that the data encryption functionality and procedures used with removable media have been implemented correctly, are of appropriate strength and fit for purpose.

5.4.3 All incidents involving the use of removable media or data encryption must be reported to the Head of IT immediately and in accordance with the Trust incident reporting procedures.

5.4.4 The Head of IT is responsible for ensuring that the Southern HSC Trust has adequate supplies of all removable media and data encryption software that has been approved for use by qualifying staff.

5.5 Role Of Senior Management

5.5.1 It is the responsibility of all Trust Directors, Assistant Directors, Service Heads and senior managers to ensure that staff comply with this policy in regard to transfer of electronic data either on removable media or through the use of data encryption.

6.0 Legislative Compliance, Relevant Policies, Procedures and Guidance

6.1 Staff must take cognisance of relevant professional standards and guidance and other Department of Health, Social Services and Public Safety publications.

6.2 Staff must always refer to the following IT Policies:

- ICT Security Policy
- Email Policy
- Encryption of Emails (Guidance)

or seek advice and guidance from the IT Department if in any doubt of their responsibilities.

7.0 Equality and Human Rights Considerations

7.1 This policy has been screened for equality implications as required by section 75, Schedule 9 of the Northern Ireland Act 1998. Using the Equality
Commission’s criteria, no significant equality implications have been identified. This policy will not therefore be subject to an equality impact assessment.

7.2 This policy has been considered under the terms of the Human Rights Act 1988 and was deemed to be compatible with the European Convention Rights in that Act.

7.3 This policy will be included in the Trust’s register of screening documentation and maintained for inspection as long as it remains in force.

8.0 Policy Approval

8.1 During development this policy was considered in draft form by Head of IT and Assistant Director of Informatics and was circulated to senior IT Staff for consultation.

9.0 Sources of Advice and Further Information

9.1 Staff should refer to the following IT related policies:

- ICT Security Policy
- Email Policy
- Encryption of Emails (Guidance)

Appendix 1 – 4 attached which provides specific detail on all aspects of Removal Media, Data Encryption, Courier Transfer and Laptop Security.

Employees who have any concerns regarding work related personal / sensitive information on a personal device, including personal computers, laptops, smartphones and memory sticks should contact the IT Department on 028 3861 3600, for advice on deleting personal / sensitive work related information from devices.

10.0 Copyright

10.1 The supply of information under the Freedom of Information does not give the recipient or organisation that receives it the automatic right to re-use it in any way that would infringe copyright. This includes, for example, making multiple copies, publishing and issuing copies to the public. Permission to re-use the information must be obtained in advance from the Trust.
11.0 Alternative Formats

11.1 This document can be made available on request in alternative formats, e.g. plain English, Braille, disc, audiocassette and in other languages to meet the needs of those who are not fluent in English.
Appendix 1

Removable Media

- Removable media shall only be used by staff and contractors who have an identified and agreed business need for them. External contractors will sign a Data Access Agreement prior to gaining access to any patient identifiable or confidential data.

- The use of removable media by sub-contractors or temporary workers must be risk assessed and be specifically authorised by the Head of IT;

- Removable media drives, that may include USB ports, are enabled and managed by appropriate firewall software. Only approved encrypted USB pens can be used in Trust PCs – this has been implemented following SMT approval to remove the risk associated with data transfer in August 2011.

- Each Directorate shall identify to the Head of IT its need for removable media and the devices on which removable media are to be used;

- Removable media that have been approved for use within the Trust will be appropriately identifiable as such, and will be asset tagged;

- Removable media may only be used to store and share Trust information that is required for a specific business purpose;

- When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file. The IT Department can provide advice in this respect, if necessary;

- Removable media must be physically protected against loss, damage, abuse or misuse when used, where stored and in transit;

- Data archives or back-ups taken and stored on removable media, either short-term or long-term, must take account of any manufacturer’s specification or guarantee and any limitations therein;

- Audit spot checks will be conducted by the Trust to ensure this policy is complied with. Any compliance issues will be reported to the line managers concerned and may be handled through staff disciplinary processes.

- All incidents involving the loss of removable media must be reported to the Head of IT immediately and in accordance with the organization’s incident reporting procedures and in line with data breach guidelines the Information Governance Team should be notified.
Appendix 2

Data Encryption

- Data intended for processing on removable media must be considered for its sensitivity and potential impacts if lost, stolen or otherwise compromised. A risk assessment in accordance with DHSS Information Governance guidance and organisational policy will determine if that data should be encrypted. This will be facilitated by the IT Department;

- Where the data is to be encrypted, an encrypted file may be created on the removable media through the application used for processing where this contains relevant encryption capability (or) through the use of an additional security product with this encryption functionality. Such products may include ones that can be used to create self-decrypting archives (SDAs) and others that encrypt data files automatically when copied to removable media. This will be provided via the Trust IT Department;

- Staff should be trained in the use of encryption tools or application facilities provided, and for the handling of encrypted removable media. These should be defined locally and may vary according to the products, facilities and removable media in-use;

- Where encrypted removable media is to be shared, care must be taken to ensure that the intended recipient has the correct technical capability to decrypt the data on receipt and this should be established in advance of any sharing of media;

- The pass-phrase or decryption key used for encryption/decryption purposes must be sufficiently long and complex to prevent the encrypted information from attack. The decryption pass-phrase or key must never be sent with encrypted removable media. This is the responsibility of the IT Department. However, all staff have a responsibility to ensure that they only use encryption software provided by the Trust’s IT Department;

- Encryption products that benefit through independent evaluation of their claims and capabilities are to be used.

- Audit spot checks will be conducted by the IT Security Team to ensure this policy is complied with. Any compliance issues will be reported to the line managers concerned and may be handled through staff disciplinary processes or contractual arrangements.

- All incidents involving the loss of encrypted data must be reported to the Head of IT immediately and in accordance with the organization’s incident reporting procedures and in line with data breach guidelines the Information Governance Team should be notified.
Appendix 3

Transfer of Data via Courier Services

Routine Courier Transfer

Routine courier services should only be used for the transfer of non-personal or non-sensitive information only

- Authority to use courier service must be obtained from appropriate level of management (Assistant Director or Director level).

- Courier is selected from contracted or authorised list.

- A telephone call is made from the Trust to the intended recipient at the receiving organisation to notify despatch

- Information for despatch is placed in a sealed envelope or wallet.

- A signature sheet is signed by despatching and receiving organisations.

Secure Courier Process

Secure courier services should always be used for the transfer of person identifiable or sensitive information

- Authority to use courier service is obtained from appropriate level of management (Assistant Director or Director level).

- Only authorised courier services used

- A signature sheet is used to capture details of handover/takeover of the data disks.

- The data file creation is authorised (name/role/date/time).

- The data file is created by (name/role/date/time) and is burned to DVD/CD and encrypted in accordance with Trust Data Encryption procedure (see Appendix 2 – Data Encryption).

- Packaging is checked to ensure it is sufficient to protect the contents from any physical damage likely to arise during transit such as exposure to heat, moisture or electromagnetic fields;

- The identification of courier is checked before handover of media
- The courier collects the encrypted disk and the signature sheet is signed by both parties.

- A telephone call to notify despatch is made from the despatching organisation to a named individual in the receiving organisation. The data disks are couriered directly to the destination.

- Nominated staff at the destination receives the disks and sign the signature sheet.

- To ensure the safety of data in transit the pass phrase should be communicated to the recipient separately from the encrypted data so that the intended recipient is the only one able to decrypt the data.

- The recipient decrypts data with the received pass-phrase and confirms that the data can be used by the appropriate database applications.

- The disks are sent back to the Trust via the secure couriers with appropriate signatures for destruction.
Appendix 4

Laptop Security

- Traditional password protection on a laptop offers limited defence against a determined attacker because the attacker has unconstrained access to the physical device. Modern complex password techniques offer more protection but are not currently on widespread use.

- The physical security controls that are possible within Trust facilities are not available outside of that environment; therefore if procedural and personal controls of the laptop are breached the only effective technical measure that can be applied is cryptography.

- Encryption products are not difficult but must be used correctly in accordance with defined procedures, in particular the password and any token must be kept separate from the laptop; these are effectively the encryption key. Data is therefore only protected by encryption when the laptop is powered off and not in normal use.

- Responsibility for the security of Southern HSC Trust laptops and their data should be assigned to individuals and tracked alongside the employment status of those individuals.

- The installation and configuration of laptop security functionality, including access control, encryption, BIOS settings, WiFi and tamper resistance will only be undertaken by the IT Department.

- All laptop users must ensure that laptops are physically secured when unattended (a security cable is provided with laptops upon request).

- Users of laptops must be given appropriate training and instruction in the use of the laptop and its security functionality. This should include their responsibility for safeguarding the laptop and their obligation to comply with relevant information governance security procedures of the Trust.

- The Trust IT Security Officer should regularly review the Trusts laptop estate to ensure that they continue to meet these requirements and that the residual level of risk from their use is acceptable.

- Regardless of a laptop’s ownership, the use of any equipment outside the Trusts business premises for the processing of Trust information must be authorised by the relevant Director or Head of Department.

- Where the processing of Trust patient information is proposed on laptop devices additional authorisation must be obtained from the relevant Director or Head of Department and security advice sought from the Head of IT.
• It is recommended that laptops, even when protected by disk encryption, should not be left in the care of any person who is not trusted to protect the information it contains.

• Continued availability of laptops, for operational reasons and because of the costs of replacement, will mean that consistent standards of physical and procedural protection will be required for all laptops used by the Trust.

• Remote access from a laptop to the Trust information systems must be achieved in accordance with the Business Services Organisation (BSO) policies and HSC Code of Connection.

• Sensitive data, including that relating to patients, stored on a Trust laptop should be kept to the minimum required for its effective business use in order to minimise the risks and impacts should a breach occur.

• Loss of a Trust laptop should be reported immediately to the IT Service Desk or Head of IT.

• Data stored on Trust laptops should be securely erased before the laptop is reassigned for another purpose or disposed of when redundant.