LUTON & DUNSTABLE UNIVERSITY HOSPITAL

CLINICAL EXCELLENCE, QUALITY & SAFETY

THIRD PARTY DATA PROCESSING AGREEMENT

Please note:
Where necessary, Third Party Contracts are underpinned by a 'Service Specific' Third Party Data Processing Agreements. It is the responsibility of the contractor to ensure they are aware of which Data Processing Agreement they are required to comply with.

ALL contractors are required to ensure that they, their staff, agents and agreed sub-contractors comply with this agreement and the Trusts **Third Party Confidentiality Code of Conduct** - see appendix A.

This Agreement:

- Underpins the contract that Third Party Contractors have with Luton & Dunstable University Hospital NHS Foundation Trust (the Trust).

- Highlights the responsibilities of the Third Party who, under the Terms and Conditions of their contract with the Trust (and where applicable their legal obligations as Data Controllers), are required to ensure that their *processing of personal identifiable data (**PID) is in line with legal, statutory and NHS requirements and obligations.

- Applies to all PID provided by the Trust, or obtained by the Contractor from other sources as part of the delivery of the contract.

**Processing - Defined in the Data Protection Act 1998 as viewing, transferring, obtaining, using, collating and storing.*
** * Personal identifiable data (PID) is data that could be used to identify an individual e.g. name, address, date of birth or NHS Number or information that could be used with other information to identify an individual including images and recordings*.

The Contractor (and any agreed sub-contractors of the Contractor) agrees to:

1 General:

1.1 Comply with ALL aspects of the Data Protection Act 1998 (DPA), Human Rights Act (HRA) and common law duty of confidentiality in relation to the processing of ALL data under this agreement.

1.2 Use appropriate technical and organisational measures to protect the PID from accidental, deliberate or unlawful disclosure, loss, damage, destruction or unauthorised access or processing.

The technical and organisational measures adopted must be in line with the requirements of:

- o ISO27001as appropriate to the services being provided
- o The Department of Health Information Governance Toolkit
- o The Data Protection Act

1.3 Keep their Data Controller Notification with the Information Commissioners Office (ICO) up to date.

1.4 Process the PID to which this agreement applies in accordance with the Data Protection Act 1998 and solely under instructions from the Trust.

1.5 Treat the PID and any other information provided by the Trust as confidential and not disclose it to a third party in any circumstances other than at the specific written request of the Trust, unless the disclosure is required by law.

1.6 Promptly assist the Trust with all Subject Access Requests which may be received from the Data Subjects of the Personal Data.

1.7 Not sub-contract any of the processing (excluding any listed in the contract) without explicit written agreement from the Trust.

Where permission is given to the Contractor to sub-contract, the Contractor will ensure that any sub-contractor it uses to process PID complies with the terms of this agreement.

Where a sub-contractor is used, the Contractor agrees that the Trust may, upon giving reasonable notice carry out compliance audits and checks of the sub-contractor to ensure adherence to the terms of this agreement.

1.8 Not sub-contract any of the contracted service/s with the Trust without the prior written permission of the Trust. Where permission is given the contractor is required to ensure the sub-contractor complies at ALL times with this agreement, the legal framework and NHS requirements in relation to Data Protection, Confidentiality and IT Security.

1.9 Ensure that any Trust data in its possession is destroyed as soon as the purpose has been achieved - see destruction below.

1.10 Not cause or allow any PID to be transferred to any territory outside the European Economic Area without the prior written permission of the Trust.

2 Employees:

2.1 Undertake all reasonable background checks to ensure the reliability of all employees who are likely to process the PID to which this agreement applies and include appropriate confidentiality clauses in employments contracts.

2.2 Ensure that all employees used by it to provide the contracted service have undergone training in the law of data protection, their duty of confidentiality under contract and in the care and handling of PID.

2.3 Ensure that ALL relevant staff are aware of, understand and comply with the requirements of the Trusts **Confidentiality Code of Conduct** (For Third Party Contractors/Suppliers) See appendix A.

2.4 Ensure only those staff who are trained to understand and comply with this agreement partake in any processing to which this agreement applies.

2.5 Ensure that access is based on a strict ‘need to know’ basis and that anonymised data or redacted extracts are used whenever possible.

3 Security - Physical:

3.1 Ensure that ALL PID processed under this agreement is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

3.2 Ensure that its premises are adequately protected from unauthorised entry and/or theft of any documents or IT equipment which the data under this agreement may be held on.

4 Security – IT Systems:

4.1 Ensure Trust PID electronically processed under this agreement is done so on secure servers.

4.2 Under no circumstances store PID on encrypted or unencrypted portable media devices e.g. laptops, USB memory sticks or CD-ROM unless agreed in writing by the Trust.

4.3 Ensure its employees do not store any PID or other Trust data on their own personal computers.

4.4 Ensure adequate back-up facilities are in place to minimise the risk of loss or damage to the PID being processed.

4.5 Not transmit PID by email except as an attachment encrypted to 256 bit or from an nhs.net email account to an nhs.net email account.

4.6 Not make printed paper copies of PID unless it is absolutely necessary and justified as the only option. Where the need for printed copies is necessary and justified they must not be removed from the premises and must be stored under lock and key when not in use.

4.7 Ensure that only its employees who require access to the PID to enable delivery of the contracted service are provided access to it and that access is controlled, auditable and audited.

5 Secure Destruction:

5.1 On satisfactory completion of the service or on termination of the contract, ensure that the PID is securely removed from their systems and any printed copies securely destroyed. In complying with this clause, electronic copies of the personal data shall be securely destroyed.

5.2 ALL PID held in paper form regardless of whether as originally provided by the Trust or not is destroyed using a cross cut shredder or by a confidential waste company that complies with European Standard EN15713 and performs shredding services on the premises.

5.3 Electronic storage media used to hold or process the data is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk. In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.

6 Auditing Compliance

Assist the Trust in carrying out compliance audits and checks to ensure adherence to the terms of this agreement in order to satisfy itself that the this agreement is being complied with.

7 Indemnities

Indemnify the Trust against any costs, expense, including legal expenses, damages, loss, liabilities, demands, claims, actions or proceedings that the Trust may incur as a result of any breach of this Agreement by the contracted company or organisation.

LUTON & DUNSTABLE UNIVERSITY HOSPITAL

CLINICAL EXCELLENCE, QUALITY & SAFETY

Appendix A

Name of Document:	**Third Party Confidentiality Code of Conduct** (For Third Party Contractors/Suppliers)
Author:	Information Governance Manager
Document created in consultation with:	Director of IM&T & SIRO Medical Director & Caldicott Guardian Interim Contracts Manager
Version:	V2 – July 2013
Date to be Reviewed:	July 2014

Content:

1. Introduction

The Luton and Dunstable University Hospital NHS Foundation Trust (the Trust) is committed to the delivery of first class confidential services.

The Trust and its staff (including any organisation or individual working for or on behalf of it) have contractual and legal obligations to comply with all appropriate legislation and guidance in respect of the privacy, security and protection (collectively known as Information Governance) of the personal identifiable data (PID) it processes, including (but not limited to):

- Data protection Act 1998
- Computer Misuse Act 1990
- The Human Rights Act 1998 (Article 8 – the right to a private life)
- Common Law of Confidentiality
- NHS Confidentiality Code of Practice

These require PID to be processed lawfully, fairly and as transparently as possible and in line with the legal rights of the 'Data Subject' (the individual the PID relates to).

2. Purpose

The Trust has a framework in place to ensure it meets its duties and obligations in relation to Information Governance (IG). This includes a series of policies, procedures and guidance documents that define the working practices the Trust and its staff (including any organisation or individual working for or on behalf of it) must adhere to ensure compliance.

The purpose of this Code of Conduct is to define the specific working practices that Third Party Contractors (NHS and non NHS organisations) and their staff/agents that are/will be, processing PID for and on behalf of the Trust **MUST** adopt.

3. Scope

This Code of Conduct applies to all Third Party Contractors and its staff/agents working for and on behalf of the Trust, regardless of whether they are working on or off of the Trusts premises. Compliance with it is a requirement of the contact and Data Processing Agreement to which the Contractor has signed up to and agreed to comply with. Non compliance with may result in the termination of that contract.

4. Data Protection Act

The Data Protection Act 1998 (DPA) is a key legislation in relation to PID as it dictates:

- what purposes it can be obtained and processed for
- who it can be disclosed to and shared with,
- how long it should be kept and,
- states that appropriate technical and organisational measures are put in place to protect it
  from unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

The ICO (the organisation who enforces the DPA) have the power to fine organisations up to £500,000.00 for serious breaches of the DPA. All offences under the DPA are criminal offences so can lead to imprisonment of individuals.

5. Your responsibilities

You are responsible for ensuring you:

- read, understand and comply with this document

- report any breaches – see section 12 below.

6. Processing & Disclosure
The access you have to NHS & Trust PID is solely for the purpose of delivering/providing the service you or your organisation are contracted to provide/deliver, and for no other purpose.

You must NOT access or process that PID for any other reasons and MUST NEVER divulge to others, information you have learnt about other individuals during the course of your duties.

7. Paper Documents containing PID
Documents containing PID e.g. health records, letters, reports etc MUST not be diclosed or removed from the Trusts premises without written consent and security instructions from a senior member of Trust staff.

8. IT Security
You MUST not use your personal/home computer for downloading or viewing PID without the prior written consent of the Trust.

You must not save documents containing PID directly to a desktop. If the computer or laptop is stolen the thief will have direct access to the documents even if it is encrypted.

Passwords for the systems you are provided access to are for your use only, they must not be written down or shared with others. If you share your password you will be responsible for what they do (audit trails are monitored regularly).

The access you are provided with will be relevant to the role you are performing and the PID you have access to will be in line with the requirements of your role

9. Laptops, Memory & Portable Devices
PID MUST never be saved on personally owned devices or devices issued to you by your organisation without the prior written consent of the Trust. Where consent is provided you will be expected to comply with the Trusts Mobile Devices Policy - please request a copy from the IT Department.

Mobile devices issued to you by the Trust will be encrypted as password protection is NOT sufficient security for mobile device (e.g. laptops, USB Sticks, iPads etc) which contain PID..... they will be encrypted to NHS standard.

Trust issued and personally owned mobile devices should be locked away when not in use.

10. Remote Working
Where the Trust grants "Remote Access" permission to an individual for the purpose of accessing any part of the Trusts network or systems, they MUST comply with the following:

- NOT to share their access right with others.
- NOT access remotely from public places (trains, airports, cafes etc.)
- NOT access remotely via the use of public computers (libraries, internet cafes etc.)
- NOT transfer or transmit ANY PID outside the EEA without the written permission of the Trust

11. Safe Haven and General Confidentiality Procedures

To ensure the security of Data Flows, the following Safe Haven procedures for transferring, transmitting and communication of PID MUST be adhered to:

11.1 Secure emailing:

Emailing – using "nhs.net":

- Emails containing PID MUST ONLY be sent using an nhs.net account AND MUST be sent to an nhs.net account or another secure email account, these are email accounts which end with **gsi.gov.uk - gsx.gov.uk - gcsx.gov.uk - gse.gov.uk - pnn.gov.uk - scn.gov.uk - pnn.police.uk - eu-admin.net - gsisup.co.uk - cjsm.net - psops.net**.
- Organisations that have connection to the N3 network (this is the secure NHS network) should be able to apply for an nhs.net account. Please go to www.nhs.net.uk for further information.

Emailing – using encryption

- When emails containing PID cannot be sent to and from nhs.net accounts or another secure email address (listed above) PID MUST be sent as an encrypted attachment. The encryption MUST be 256 bit encryption.

Emailing – using "ldh.nhs.uk"

- Emails can be sent from an ldh.nhs.uk account to an ldh.nhs.uk without encryption.

Emailing – general

- Do not include PID in the subject field
- Distribution lists must be regularly updated to ensure only relevant individuals are included.
- ALWAYS double check the email address to ensure you are emailing the correct person.
- NEVER send emails containing PID to or from web accounts e.g. hotmail etc

11.2 Faxing

Do not fax PID unless it is absolutely necessary and only if you have permission from a senior member of Trust staff. *Faxes being sent to the wrong number are one of the biggest causes of breaches of confidentiality.*

Where faxing is necessary and approved by a Trust Manager, the following 3 steps must be followed:

Step 1:

Ensure you use a Safe Haven front sheet - internally, these are available on the Intranet. (A Safe Haven Front Sheet Must be a sheet of headed paper marked as **'Private & Confidential'** and contain no PID, but include your name, contact telephone and the fax number you are sending from, the name, organisation and fax number you are sending to, the number of pages included in the transmission including the front sheet).

Step 2

Call the recipient to let them know you are sending them a fax and to double check their fax number. (Do not rely on number that have been programmed into machines unless you are 100% sure that number is still correct).

Step 3

Ask the recipient to confirm they have received the fax, or call them back to make sure they have received it. (Do not rely on fax receipts).

- If you are not in a position to be able to speak to the intended recipient/organisation you should remove (blank out the individuals address), if it is not required.
- The fax MUST be addressed to an individual or team.
- Fax machines should be sited in areas that are restricted to only those who need to access it.

11.3 Post

- Ensure that incoming post is opened in private and NOT on view in a public area or where is can be seen by individuals who do not have a legitimate right to see it. Post trays MUST be placed out of the reach of the public.
- Normal sealable (external) envelopes MUST be used for sending ALL post that contains PID - envelopes MUST be marked **'Private & Confidential'**. Internal envelopes MUST NEVER be used for sending documents containing PID.
- Double check what you are inserting into the envelope to ensure other documents have not been picked up and included by mistake.
- Should it be sent using regular postal service or should it be sent Recorded or Special delivery?... discuss options with the Trust. Thought should be given to how sensitive the information is that you are sending and how many individuals confidentiality would be breached if the letter/parcel went to the wrong person. Is the address correct? When was it last updated/checked?

11.4 Telephone Calls & other conversations

- When receiving calls from individuals requesting information always verify the identity of the caller and ask why they require the information. If in doubt about the identity of the caller tell them you will call them back. Call back to main switchboard or known and trusted numbers only – not direct lines you do not recognise or mobile numbers. If in doubt speak to your Manager and report any suspected "Bogus" calls to the Trusts IG Manager.
- Always make calls in private Safe Haven locations.....never in public areas.
- Be careful about leaving messages on answer phones. Did you call the right number??..... when listening to messages left on answer phones ensure they cannot be overheard.

12. Incident Reporting

All incidents relating to actual or potential breaches of confidentiality involving PID, must be reported <u>immediately</u> using the Trusts incident reporting mechanisms. Where this is not possible the incident must be reported directly to the Trusts IG Manager without delay.

Incidents which constitute a breach of confidentiality include, but are not limited to:

a) Sharing of passwords to access IT Systems which contain PID
b) Documentation sent (by email, post or fax) in any form/media to the wrong individual or organisation.
c) Accidental loss or destruction of PID (in any format) e.g. lost or misplaced documents.
d) PID divulged during a conversation with the wrong person.
e) Photographs or any other recording of individuals without their consent.
f) Access to or sharing of PID without the approval of the Trust.
g) Inappropriate use or disclosure of PID.
h) Theft of any paper or equipment containing PID.
i) Documents or equipment containing PID which are found in a public or inappropriate place.
j) Any use of PID not compatible with the service being provided under the contract.

13. Further Information

For further information about Information Governance and Data Protection/Confidentiality requirements, please contact the Trusts IG Manager.