INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

<table>
<thead>
<tr>
<th>PROCEDURE NUMBER:</th>
<th>CPG50D</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>1</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION:</td>
<td></td>
</tr>
<tr>
<td>AUTHOR:</td>
<td>Information Governance Team</td>
</tr>
<tr>
<td>CONSULTATION:</td>
<td>Information Governance Steering Sub - Committee;</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>April 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td></td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>July 2018</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>July 2021</td>
</tr>
<tr>
<td>APPROVAL BY INFORMATION GOVERNANCE &amp; SECURITY SUB-COMMITTEE:</td>
<td>September 2018</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE</td>
<td>N/A</td>
</tr>
<tr>
<td>COPYRIGHT</td>
<td>© Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner</td>
</tr>
</tbody>
</table>

POLICY SUMMARY

The purpose of these procedural guidelines is to establish the governance arrangements and responsibilities for information security providing a framework through which the elements of information governance / security will be met. This will make sure that the intention to promote and build a level of consistency across the Trust to safeguard information is achieved and ensure it is understood and that all Trust staff are aware of their individual responsibilities.

The risk associated with not having a procedure document in relation to information governance / security and access to Trust facilities (IT, Email, Internet, and Portable Media) is an uncoordinated approach to its safe use which could render the Trust vulnerable in terms of legal implications of staff use of facilities and lack of organisational controls to safeguard users and the Trust.

The Trust monitors the implementation of and compliance with this policy in the following ways:

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. Incidents will be managed through the Trust Datix System.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
The Executive Chief Finance Officer
CONTENTS

1.0 INTRODUCTION

2.0 RESPONSIBILITIES

3.0 REPORTING PROCEDURES

APPENDICES

APPENDIX 1 – SECURITY INCIDENT OPENING REPORT FORM

APPENDIX 2 – INFORMATION SECURITY INCIDENT INVESTIGATION FORM

APPENDIX 3 – CLASSIFICATION OF INFORMATION GOVERNANCE / SECURITY INCIDENTS
Assurance Statement

This procedure aims to ensure that all Trust staff are aware of the procedures that need to be followed in the event of an information security incident / information confidentiality breach and that risk of disruption to the Trust’s operations are minimised.

This procedure is linked to the Adverse Incident Policy and Procedures and should therefore be read in conjunction with CP3 & CPG3.

1.0 INTRODUCTION

1.1 An information security incident (Incident) / information confidentiality breach (Breach) is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the computer system or data being put at risk
- The availability of the computer system or information being put at risk
- An adverse impact, for example:
  a) Threat to personal safety or privacy;
  b) Legal obligation or penalty;
  c) Financial loss;
  d) Disruption of Trust business; or
  e) An embarrassment to the Trust.

2.0 RESPONSIBILITIES

2.1 All staff have a responsibility for reporting security Incidents / Breaches.

2.2 The Trust’s Executive Chief Finance Officer (Senior Information Risk Owner) and the Executive Medical Director (Caldicott Guardian) are the Directors responsible for information security / confidentiality and with the Information Governance Manager are responsible, for implementing, monitoring, documenting and communicating information security within the organisation, in compliance with all UK legislation and national policy and guidance.

2.3 The Data Protection Officer and the Information Governance Manager are responsible for:

- Monitoring and reporting to the Chief Executive (SIRO) the state of information security within the Trust;
- Developing and enforcing detailed policy and procedures to maintain security and ensuring that these are implemented throughout the Trust and followed;
- Ensuring compliance with relevant legislation, including the General Data Protection Regulation and Data Protection Act 2018;
- Ensuring that relevant staff are aware of their security / confidentiality responsibilities and that security awareness training is provided for all IT users;
Monitoring for actual or potential information security / confidentiality breaches within the Trust.

2.4 Trust management also has a responsibility to ensure that staff are aware of security risks and their responsibilities to minimise threats, i.e. Management should:

- Ensure that all current and future staff are instructed in their security responsibilities;
- Ensure that all staff using computer systems are trained in their use;
- Ensure that no unauthorised staff are allowed to access any of the Trust’s computer systems as such access could compromise data integrity;
- Determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function, independent of status;
- Implement procedures to minimise the Trust’s exposure to fraud / theft / disruption of its systems, such as segregation of duties / dual control / staff rotation in critical susceptible areas;
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
- Ensure that staff are aware of the Trust’s Standing Orders on potential personal conflicts of interest;
- Ensure that all staff sign confidentiality (non-disclosure) undertaking as part of their contract of employment; and
- Ensure that the relevant systems managers are advised immediately about staff changes affecting computer access so that passwords may be withdrawn / deleted.

### 3.0 REPORTING PROCEDURES

#### 3.1 Overview

3.1.1 All incidents / breaches or information indicating a suspected (near miss) or actual security breach should initially be reported to the immediate line manager.

3.1.2 The majority of breaches are innocent and unintentional (e.g. user not ‘logging out’ when leaving for the day) and would not normally result in disciplinary action being taken.

3.1.3 All incidents whether they are actual or near misses must reported by staff within 48 hours of the incident using the appropriate web based Datix Incident Reporting Form. The Information Governance Team, will determine whether an actual breach has taken place.

3.1.4 The Information Governance Team will categorise the incident / breach within one of the classifications (from insignificant to acute) as defined in the NHS Executive’s Incident Classifications Table.
3.1.5 The Information Governance Team will report all Level 2 incidents / breaches to the ICO.

3.1.6 All incidents / breaches that may have an impact on NHS.net will be reported immediately, by the Information Governance Team, to the Regional Telecommunications Branch Security Coordinator or NHS.net Security Manager.

3.1.7 The information Governance Team shall maintain a record of all reported incidents / breaches which will be reported to the Trust Board and Caldicott Guardian at regular intervals.

3.2 Reporting Procedures if Datix is available for use.

3.2.1 Datix is a dedicated risk management software that provides a joined up approach to risk management and compliance against standards by bringing together Incident Reporting, Complaints, Claims, CQC Standards and Risk Registers. The link for Datix can be accessed via the Trust’s intranet home page.

3.2.2 What to expect from the incident reporting form:

The form itself is simple and is structured systematically enabling you to identify the type of incident, location, category, and contacts. All sections with a red star are mandatory and require an entry. The form has several drop-down boxes giving you a number of options to choose from.

3.2.3 Incident date and time:

A calendar will appear and this will allow staff to choose the date the incident happened and enter a time format using a 24-hour clock.

3.2.4 Area:

This option will allow staff to identify which area the incident relates to.

3.2.5 What is the name of your team, where your team is based, which service / specialism are you reporting from:

These options will allow staff to choose which team / service / specialty which contributed towards the incident or may have been involved in an incident which was committed by an external organisation. Identifying the service / specialty will allow the service / specialty lead to be notified that the incident has occurred.
3.2.6 Where did the incident occur (location), at what type of location did the incident occur:

These options will allow staff to enter the location where the incident occurred and what types the location might be (e.g. GP Practice, car park etc).

3.2.7 Describe what happened, immediate action taken:

These options will allow staff to detail the events of the incident and what action the staff member reporting the incident might have taken or the staff member’s line manager or the patient / service user / external organisation might have taken. (Note: No names, initials or place names should be used in these sections)

3.2.8 Incident classification, Additional information, Persons involved, Details of the reporter, Name of Manager

The above section will allow staff to add the incident type (e.g. Security, Procedures, Breach of Confidentiality etc.) and any additional information which might be relevant to the reporting process. Details of persons related to the incident need to be entered to allow the investigating officer the option to contact these persons when necessary to ensure the investigation is done correctly and according to policy.

(Note: For any queries or comments about the e-Form, please contact the Risk Management Department)

3.3 Reporting Procedures if Datix is not available for use.

3.3.1 An unusual incident or significant security breach must be reported on an Incident Opening Form (see Appendix A). The form must be completed by either the Reporting Officer or their line manager and forwarded to the Risk Management Department.

3.3.2 The Information Governance Team are responsible for ensuring that the Incident Opening Form is completed where deemed appropriate and that, at the same time, an Incident Investigation form is opened (see Appendix B).

3.3.3 The Information Governance Team must maintain a log of all Incident Opening and Investigation forms completed.

3.3.4 Incidents must remain open until the ‘Cause and Action’ section of the incident investigation form is completed to a satisfactory conclusion. As soon as is possible during the course of the investigation the Information Governance Team must categorise the incident / breach within one of the categories (from Insignificant to Acute) as defined in
the Classification of Incident table in Appendix C. The incident / breach may need to be re-categorised during the course of the investigation as new information or impacts are discovered.

3.3.5 If the security breach is defined as Significant, Major or Acute then the SIRO / Caldicott Guardian must be informed immediately and fully briefed at the first opportunity.

3.3.6 Where the incident / breach impacts on the Trust’s computer, network, server delivery the Information Governance Manager is responsible for fully briefing the Associate Director of IT and / or the Associate Director of Electronic Systems and IG on all aspects of a Significant, Major or Acute incidents / breaches.

3.3.7 Any staff member reporting a breach of IT security must have unhindered access to the Associate Director(s) of Electronic Systems and IG if that staff member believes the breach has been as a result of an action by the Information Governance Manager.

3.3.8 The Information Governance Manager is available to any member of staff reporting a breach in information security. The anonymity of the member of staff must be ensured, irrespective of whether or not the event turns out to be a genuine breach or a false alarm. It is most important that the reporting process is made as easy as possible, especially where the offence is being committed by someone in a position of trust. It is possible that the offender may be in a position of authority over the staff member making the report. Therefore, it is essential that no adverse pressures are brought to bear on the staff member as a consequence.

3.3.9 The Information Governance Team are responsible for ensuring that documented records of incidents are retained and stored securely for audit review.

END