Tower Hamlets GP Care Group
Information Security Policy

Date Issued	September 2017
Date to be reviewed	Periodically or if statutory changes are required
Title	Information Security
Supersedes	All previous Policies
This policy will impact on	All staff
Financial Implications	No change
Policy Area	Information Governance
Version No	4.0
Issued By	Ruth Walters
Author	Ruth Walters
Document Reference	
Effective Date	01/10/2017
Review Date	April 2019

Approval Record

	Committees / Groups / Individual	Date
Consultation	Quality, Safety & Governance Committee, THGPCG Board	August 2017
Approved by	Dr Joe Hall, Chair, Quality, Safety & Governance Committee	September 2017

Information Security Policy

INTRODUCTION

1. The security and confidentiality of information, in both paper and electronic form, is central to all aspects of the THGPCG's work. The protection of the organisation's information assets from all threats – whether internal, external, deliberate or accidental – will help to ensure that information is readily accessible to support better care for all patients.

2. A failure to follow the requirements of the guideline may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the THGPCG's disciplinary or capability procedures for employees, and other action in relation to organisations contracted to the THGPCG, which may result in the termination of a contract, assignment, placement, secondment or honorary arrangement.

3. The effective application of this policy will help to ensure that:
   - Activities relating to the use of information meet legal requirements
   - All THGPCG information systems and assets are secure and confidential, with appropriate protection from unauthorised access.
   - Accountability and responsibilities for information security across the THGPCG are clear.
   - All staff are aware of the policy and their responsibilities in maintaining the integrity and security of information.
   - There is a risk management process in place to ensure that all recognised threats are evaluated.
   - Actual or potential breaches of information security are reported and investigated in an appropriate manner.

SCOPE OF POLICY

4. The policy covers the security of all information managed by the THGPCG, in both paper and electronic format.

5. While key individuals within the THGPCG have specific duties in relation to certain parts of this policy, adherence to the policy is mandatory for all staff and others who have access to information and systems.

KEY REQUIREMENTS

6. Trust employees, contractors or volunteers, including honorary contract holders, are prohibited from installing any computer equipment, mobile communication device or other connection to the THGPCG's network without approval.

7. Staff must always lock their computer when leaving it unattended. (N.B. the **'Ctrl+Alt+Del'** key sequence enables users to lock their computer; 'Ctrl+Alt+Del' unlocks a computer on entry of the password).

8. Staff should not leave any patient-identifiable or other confidential information unsecured or unattended in any area. Lockable cabinets should be used to store patient-identifiable information and these should be locked when not in actual use.

RESPONSIBILITIES

9. The Information Governance Lead and the Service Leads have responsibility for the day-to-day management of information security in the organisation

10. The Chair of the Governance Committee has overall responsibility for the implementation of the organisation's Information Security policy.

11. The Chief Executive is responsible for the security and protection of the Trust's ICT assets.

12. The Chief Executive, as the Trust's Senior Information Risk Owner (SIRO), will act as an advocate for information risk at Board level and ensure that identified information security risks are followed up and incidents managed. The SIRO will also ensure that the Board is updated on key information risk issues and will provide written advice to the Accountable Officer on the content of their annual Statement on Internal Control (SIC) in regard to information risk.

13. Information Asset Owners (IAOs) will be assigned to each of the organisations's main information assets and will ensure that information risk assessments are undertaken at least annually on all information assets where they have been assigned 'ownership'. These will be based on guidance issued by the SIRO covering the assessment methodology, format and content. IAOs will submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. This process will be administered by the Head of Information Governance.

14. All staff have a responsibility to maintain the integrity, confidentiality and security of THGPCG information and to ensure that they are familiar with the requirements of this and the related policies.

CONFIDENTIALITY OF TRUST INFORMATION

15. Many THGPCG records contain person-identifiable or other sensitive or confidential information. It is therefore essential that the security and confidentiality of information is safeguarded at all times. All staff should be aware of how easy it is to breach confidentiality by inappropriate use, storage and disposal of information.

16. Staff should ensure that they adopt whenever possible a clear desk/work area and screen policy:

    - *Clear Screen* - computer screens must be positioned so that person-identifiable and other confidential or sensitive information is not inadvertently disclosed to someone who does not have the right or need to see the information.
    - *Clear Desk/Work Area* - staff should ensure that desks and other work as are clear of person-identifiable and other confidential or sensitive information when left unattended or that the area is secured.

17. Staff should not be keep patient-identifiable or other confidential or sensitive information in their personal possession for any longer than is necessary for providing patient care or related activities

18. When not being used by a member of staff for such purposes, the information should be filed on a patient's health record or in a secure Trust filing system as appropriate, or disposed of securely if not required as part of the record.

19. Staff should dispose of paper copies of person-identifiable or other confidential information by placing the information in a locked confidential waste bin or by shredding the information.

20. In no circumstances should such information be disposed of in any other way.

21. In any circumstances where it is necessary for patient care reasons for a member of staff to carry patient-identifiable information between clinical areas or outside THGPCG premises, such information must never be left unattended by the member of staff and must be returned immediately after use to the patient's health record or a secure filing system as appropriate.

22. No person-identifiable or other confidential or sensitive information should be left unsecured or unattended in any area. Lockable cabinets should be used to store such information wherever possible and these should be locked when not in use. All removable computer media (including laptops, PDAs and USB sticks) should also be secured when not in use.

23. On leaving rooms containing person-identifiable or other confidential or sensitive information, staff should ensure that where possible all desks are cleared and windows and doors are locked.

24. Access to personal information should be on a need to know basis. Staff must only access information they are required to use to undertake their duties. Staff must not access any information which they do not a have legitimate reason to see as part of undertaking their role. In particular, unless it is part of their job description and required for delivering care to a specific patient, staff are not permitted to access the paper or electronic records of any patient including relatives and friends, even with their consent. **Inappropriate access to a patient's health record by a member of staff will be treated as a disciplinary offence.**

SECURE METHODS FOR TRANSFERRING INFORMATION

25. Under no circumstances must electronic data be copied from a THGPCG system unless it is to encrypted media, for a clear business purpose and for a time-limited period.

26. All external transfers of person-identifiable data (PID) must be registered and approved by the Information Governance team using the Trust's Data Transfer Form, contact the Information Governance Team for further information.

- *Electronic Transfer:* Only THGPCG-approved encrypted USB sticks or encrypted portable devices must be used to transfer information and the data must be deleted immediately after use. For bulk data transfer NHS Secure File Transfer (SFT) should be used where possible. Further guidance on SFT can be found on the Information Governance Intranet page. Detailed guidance for sending person identifiable data via email is available on the Information Governance intranet

- *Paper Transfer:* Documents must be placed in a sealed envelope, correctly addressed with sender details on the reverse and marked **Private and Confidential.**

- *Fax Transfer:* Information must be sent to a Safe Haven Fax. Extra care should be taken when sending person-identifiable or other confidential information via fax. Person-identifiable information should be anonymised wherever possible. Fax numbers must be double checked before the information is sent and where there is any doubt a test page should be sent first and its safe receipt confirmed before sending the confidential information.

LEGAL ADMISSIBILITY

27. Where legal admissibility of electronic data is being claimed, any data compression methods used during transfer of the data must be sufficient to ensure that the integrity of the documents is guaranteed both during transfer and after decompression. On receipt of a transfer the service should undertake checks to ensure the integrity and authenticity of the data that has been transferred. Specifically, to ensure legal admissibility, the appropriate decompression and decryption procedures undertaken after receipt should be documented, as well as the procedure for identification and verification of the sender (where appropriate). Procedures for the protection from malicious software

should be documented and implemented. Details of any temporary storage processes should be documented. If personal information is being transferred out of or into the organisation it must be encrypted to AES 256 bit as recommended by the Department of Health. Access to encrypted documents must be allowed only by the application of the appropriate decryption key. Access arrangements to the decryption and encryption keys must be appropriate to ensure security at all stages of the transfer and after receipt."

28. Where an electronic equivalent of a 'pen and ink' signature is required (electronic identity verification), the process for capturing this must be designed to meet the requirements of the British Standard Code of Practice: Evidential weight and legal admissibility of linking electronic identity to documents – Code of Practice for the implementation of BS 10008 (BIP 0008-3)"

29. Where legal admissibility of electronic data is being claimed, any electronic transfer systems must be audited as outlined in "BS 10008 Evidential Weight and legal admissibility of electronic information."

30. Where legal admissibility is being claimed for electronic storage and/or transfer systems, segregation of roles should be implemented in regard to quality assurance processes and approving disposal of information, to ensure additional assurance."

STORAGE OF TRUST ELECTRONIC INFORMATION

31. The THGPCG's Storage Area Network (SAN) is the primary storage resource for information held electronically. Regular back up of relevant information is undertaken every evening and stored off-site in accordance with NEL CSU Continuity Plan (SLA agreement).

32. Staff should store all THGPCG electronic information on the appropriate network drive or an approved formal records management system or database. Limited personal information should be stored on a personal network Drive. Local PC drives (typically C:/ drives including the 'Desktop') are neither secure nor backed up and data should not be stored on them.

33. THGPCG information must be stored to enable efficient retrieval and effective management of the information. Staff must set up logical folder structures to save and organise their electronic documents that can be understood by colleagues and future post holders. Each folder must have access permissions set to reflect named staff who are entitled to view/amend the content. Each of the high level/ main folders will have a named administrator who will oversee this.

34. Information will be retained for a specified period as stipulated in the THGPCG's Records Policy. Information that is no longer required should be disposed of or archived securely in line with the THGPCG Records Policy.

35. Portable devices should not be used for the permanent storage of person-identifiable or other confidential information. If being used to temporarily store such information for legitimate and necessary business purposes, such devices (e.g. laptops and USB sticks) must be encrypted in accordance with NHS standards.

36. When requested by an appropriate manager, every member of staff will be provided with a network account. The account will enable them to access appropriate THGPCG electronic information systems.

37. Staff are responsible for maintaining the security of their individual account and must not share their username and/or password with anyone or use anyone else's username and password. Passwords must be changed when prompted by the system or changed immediately if the employee believes that another person has gained access to their password.

38. Services are responsible for liaising with ICT regarding the username and password management of staff network accounts. This includes:

    - Setting up new users in accordance with THGPCG procedures.
    - Issuing original passwords.

- Deleting expired/dormant accounts.
- Removing access rights when staff leave the THGPCG.
- Undertaking regular auditing/monitoring of THGPCG systems.
- Advising users of the self-service password reset facility.

39. Passwords must:
    - Use a combination of letters, numbers, and characters.
    - Use at least 8 characters.
    - Not be revealed to anyone nor stored where anyone could see or access them.
    - Not be easy to guess (e.g. the same as your username).

40. Any member of staff who uses another member of staff's login user name and password in order:
    - to use data or a program, or
    - to alter, delete, copy or move data or a program

    is in breach of the Computer Misuse Act 1990. In this case, both the individual who borrowed the login details and the individual who provided them would be deemed to have committed an offence under the Act. Staff found sharing passwords may be subject to disciplinary action.

INTEGRITY OF TRUST INFORMATION

41. Staff must manage the information on the THGPCG's systems in accordance with the requirements of the THGPCG's Transfer and Receipt of Information Policy and Records Policy.

42. All THGPCG computer equipment has centrally controlled malware protection software. You should contact the ICT Service Desk if this is not present on the computer you are using.

43. Staff are not permitted to use personal screen savers.

44. Access to the Internet is through the THGPCG's Firewall. Staff are not permitted to access the internet using THGPCG equipment outside the THGPCG sites i.e. at home or via wireless connectivity.

45. Portable Computing Devices (PCDs) such as laptops, notebooks and PDAs should not be attached to the THGPCG Network without ICT approval. ICT will install and provide support only for THGPCG purchased PCDs.

46. Staff using approved PCDs must ensure that these devices are encrypted.

47. Staff must ensure that they take adequate precautions to ensure that PCDs are not damaged, lost or stolen. In the event that the device is stolen, staff must report the theft to the police at the earliest opportunity and obtain an incident number. Staff must also inform the ICT Helpdesk and the Information Governance Lead as soon as possible and provide an inventory of all information held on the device.

48. Staff leaving the THGPCG must return PCDs to their line manager who will be responsible for returning the equipment to ICT as appropriate.

REMOTE ACCESS SERVICE

49. ICT operate a Remote Access Service (RAS) whereby THGPCG users are able to access systems, including their network account and THGPCG intranet, when not using THGPCG networked computers.

50. All RAS users must abide by the Remote Access Protocol. Trust staff can request access to this service by contacting the ICT Service Desk.

51. To support flexible working, NHS Net allows staff to access their THGPCG email via the internet from home. The Trust recognises that some staff will also wish to access their emails using their personal mobile phone devices. However, in doing so appropriate measures need to be in place to protect the confidentiality, integrity and availability of patient and Trust sensitive information.

52. Where a member of staff chooses to use their personal mobile phone to access NHS net email, they are required to comply with the following requirements (where available):

    - The device should have the 'lock' facility activated, protected with a unique PIN code.
    - Encryption should be activated at maximum strength.
    - The device should be set to lock automatically when not in use.
    - Loss of a personal device should be reported immediately to the service provider to ensure that the device is disabled remotely. If NHS net email or other information was stored on the device, the loss should also be reported through the THGPCG's Incident Reporting Procedures.

53. For THGPCG issued devices, the loss of the device should be reported immediately to the ICT Helpdesk, who will arrange for the device to be wiped remotely, and to the Head of Information Governance. In addition, theft of devices should be reported to Service Manager.

INTERNET ACCESS

54. The THGPCG supports Internet access for work-related activities, e.g. research and training.

55. Personal use of the internet via the THGPCG network is permissible in an individual's own time subject to full compliance with this policy. Use may be restricted at the discretion of the Service Manager where such use is deemed to compromise the integrity or performance of work-related activity.

56. The THGPCG will take no responsibility for the security of any personal information disclosed by a member of staff while using the internet, e.g. credit/debit card or other financial details. Staff are advised not to supply these details, however, if they choose to do so this is at their own risk.

57. No member of staff is permitted to access, display or download from Internet sites that contain abusive material. To do so is considered a serious breach of Trust security and may result in disciplinary action up to and including dismissal.

58. The definition of "abusive" will take account of the human rights, equality & diversity in employment policy and Harassment and Bullying amongst staff Policy and refers to injurious, degrading or corrupting text or images relating to the Protected Characteristics defined by the Equality Act 2010: sex, race, age, sexual orientation, religion and belief, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership, and disability. The THGPCG Board may, at its discretion, block access to categories of websites deemed inappropriate for work access.

59. Blogging and social networking sites present an easy means for THGPCG information to inappropriately enter the public domain. Risks include unauthorised disclosure of person identifiable or other confidential information, identity theft, legal liability from defamatory postings, reputational damage, malicious code causing virus infections and system overload.

60. The THGPCG deploys technical controls to block general staff access to known social networking and blogging sites. Under no circumstances should staff engage in social networking or blogging activities on

any sites using a THGPCG PC, including any not currently blocked by the THGPCG, unless it is a direct requirement of their role for which specific access has been granted by the THGPCG Board. This includes access from THGPCG portable devices.

61. Individuals must not add any THGPCG information to their personal social networking accounts nor engage in any discussion about their work or the THGPCG which could bring the THGPCG into disrepute.

MONITORING OF TRUST SYSTEMS

62. ICT will regularly monitor storage of information on the THGPCG's servers. Members of staff with high storage levels may be asked to justify their storage of information..

63. The THGPCG has access to software that enables staff use of the internet, including access to individual websites, to be monitored at the request of line managers. Typically such requests relate to concerns about excessive use of the internet during working hours or attempts to access offensive/restricted sites.

64. The THGPCG limits the number of websites available to be accessed through the application of filters.

65. Websites that are categorised as 'non-permissible' are those that relate to:

- Advertisements and Popups
- Gambling
- Software downloads
- Tasteless and offensive
- Society and Culture
- Hacking
- Intolerance & Hate
- Criminal Activity
- Violence
- Motor Vehicles
- Weapons
- Spyware
- Proxies & Peer to Peer
- Glamour & intimate Apparel
- Personals & Dating
- Games
- Chat
- Streaming & Media (this does not apply to authorised Webinars)
- Adult/Sexually Explicit
- Phishing & Fraud

This list is not exhaustive and will be continually reviewed and updated.

66. If a member of staff needs to access a restricted website for work related purposes, they should contact the ICT Service Desk. Access to a restricted site must be authorised by the member of staff's line manager.

67. In exceptional circumstances, monitoring of a member of staff's THGPCG email account may be undertaken without the individual being informed in advance. Such monitoring, which constitutes directed surveillance as defined by the Regulation of Investigatory Powers Act (RIPA) 2000, can only take place following the written authorisation of the Chief Executive of the THGPCG or his nominated deputy. In undertaking any directed surveillance, the THGPCG will abide by RIPA, Article 8 of the European Convention on Human Rights and the Information Commissioner's 'The Employment Practices Code: Part 3 Monitoring at Work'. Requests for authorisation of directed surveillance should be made to the Chief Executive. The request and the Chief Executive's decision will be recorded in writing and held by the Clinical Governance Lead.

68. Any information, including historical information, collected during monitoring may be used to assist in assessing whether a disciplinary offence has been committed.

INCIDENT REPORTING

69. All actual or potential breaches of information security must be reported by the member of staff or their line manager through the THGPCG's Incident Reporting procedures. All Information Security Incidents must also be reported to the Information Governance Lead, who will provide expert advice to assist investigations and ensure, where appropriate, that the incident is escalated to relevant external bodies. The Information Governance Lead will also provide a summary of information security incidents to the THGPCG's Information Governance Committee on a regular basis.

ADVICE AND GUIDANCE

70. Advice and guidance on the implementation of this policy is available from the Governance Committee

APPENDIX A - LEGAL OBLIGATIONS

The THGPCG is required to adhere to the following key pieces of legislation:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- The Equality Act 2010
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2001
- Electronic Communications Act 2001
- Copyright Designs and Patents Act 1988

- Health and Safety at Work Act 1974 (Computers)

The THGPCG is also required to follow legal obligations and NHS directives listed below:

- The common law duty of confidentiality
- ISO 27001: International Information Security Standards
- The Caldicott Report: Report on the Review of Person Identifiable
- Information, Department of Health April 1998.
- The Public Records Act 1958 and 1967
- The Personal Files Act 1987
- The NHS (Venereal Diseases) Regulations 1974
- The NHS Trusts (Venereal Diseases) Directions 1991
- The Human Fertilisation and Embryology Act 1990 as amended by the Human
- Fertilisation and Embryology (Disclosure of Information) Act 1991
- Criminal Procedures and Investigations Act 1996
- Crime and Disorder Act 1998
- Health and Social Care Act 2001
- Children Act 1989 and 2004