Best Care
Healthy Communities

NHS
Birmingham
Community Healthcare
NHS Foundation Trust

Data Security and Protection Policy

BCHC Document Reference Number	CH 699

If this is a paper copy of the document, please ensure that it is the most recent version. The most recent version is available on the Intranet/internet

Title:	Data Security and Protection Policy
Version number:	Version 1
BCHC Policy Reference Number	CH 699
Is this document new or a replacement for existing? If replacement state full title and version number	Replacement of: Confidentiality and Data Protection Policy – Version 1 Information Security Policy – Version 4 Information Governance Clear Desk and Clear Screen policy – Version 3 Safe Haven Policy – Version 3
Author/Document Lead	Ben Pumphrey – Data Protection Officer
Name of Executive Director Lead:	Michelle Woodward – Director of Corporate Governance
Name of Approving Committee/Group & Date:	Information Governance Steering Group – 05/03/2019
Name of Ratifying Committee & Date:	Joint Negotiating Consultative Committee – 20.06.2019
Review Date:	05/03/2020
Date Issued:	05/08/2019
Date & Outcome of assessment for E&HRA	16.05.2019 – No adverse impacts – assessment approved
Target Audience	All staff
Subject category:	Data security and protection
Summary	This policy aims to describe the principles and legislative framework that must be observed by all who work within the Trust when dealing with confidential information and to ensure staff are aware of the need to ensure the confidentiality and security of information and that they understand and comply with any legislation referred to in this and associated policies, procedures, and guidance. Keywords: Information Governance, Confidentiality, Cyber Security, Information Security, Data Protection, Information Sharing, Records Management, National Opt- Out.

Commencement of Consultation Date

Consultation History:
The following Committees, groups or individuals have been consulted in the development of this policy:

Name:	Date:
Data Protection Officer	January 2019
Information Governance Manager	February 2019
Quality & Standards Assurance Team	February 2019
Information Governance Steering Group	March 2019
Executive Team Meeting	March 2019
EHRA review	March 2019
Joint Negotiating Consultative Committee	June 2019

Previous Version History

Version No.	Lead	Date Change Implemented	Reason for Change
1.	Data Protection Officer	March 2019	New DSP policy incorporating various preceding policies to consolidate.

Contents

1. Introduction

Birmingham Community Healthcare NHS Foundation Trust ("the Trust") needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include but are not limited to patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, date of birth, private and confidential information, and special categories of personal information.

In addition, the Trust may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (the Act). References to provisions of the Act in this policy include provisions of the GDPR which should be read alongside the Act.

The lawful and proper treatment of personal information by the Trust is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. The Trust must ensure that it processes personal information lawfully and correctly.

2. Purpose

The purpose of this policy and associated data protection policies and procedures is to support staff by setting out the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of the Trust's information. This policy is the overarching policy for data protection within the Trust and is supported by specific policies in respect of information security and confidentiality. It supports the seven Caldicott principles, the seven data protection principles and the ten data security standards (please see paragraph 2 for further details).

This policy aims to lay down the principles that must be observed by all who work within the Trust and to provide them with sufficient guidance to deal with confidential information, whether it is patient, staff or corporate information and to ensure the Trust is compliant with the requirements of the legislation surrounding confidentiality and data protection.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted, and contractors and sets out:

i. the responsibilities of all staff and third parties acting on the Trust's behalf that process, use or access confidential Trust patient, staff and corporate information and the legal implications of the use of such information; and

ii. the relevant policies and procedures in place within the Trust to allow for staff members to comply with these obligations.

Failure of compliance

Failure to comply with this policy, and any of the subordinate policies and procedures and any associated legal obligations may result in the Trust facing adverse consequences, including ICO enforcement action and / or a financial penalty and may lead to disciplinary action being taken against individuals by the Trust and potentially that individual's professional body (where applicable).

4. Objectives

4.1 Data Protection Law

On 25 May 2018, the Data Protection Act 1998 was replaced with the General Data Protection Regulation 2016 ("**GDPR**") and the Data Protection Act 2018 (the "**DPA 2018**"). While the GDPR and the DPA 2018 preserved a number of the principles enshrined in the Data Protection Act 1998, they also added some further principles. These will be considered below.

4.1.1. Data Protection Principles

- Data must be processed lawfully, fairly and transparently;
- Data must be processed for specified, explicit and legitimate purposes;
- Data must be adequate, relevant and limited;
- Data must be accurate;
- Data must be kept for no longer than is necessary; and
- Data must be processed in a manner that ensures the appropriate security.
- You must be accountable for how you handle personal data and be able to demonstrate your compliance.

In addition to the data protection principles, the GDPR also introduced further rights for individuals in respect of how their personal data is being managed by the Trust.

4.1.2 Rights of data subjects:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

4.2 Caldicott Principles

In 1997 The Caldicott Committee, chaired by Dame Fiona Caldicott developed six standards for the safe handling of patient identifiable information. In March 2013 the Information Governance Review amended these standards and added a seventh standard. The Caldicott Principles work in conjunction with the Data Protection Act and are guidelines for NHS staff when dealing with patient information. They are:

- Justify the purpose;
- Do not use personal confidential data unless it is absolutely necessary;
- Use the minimum necessary personal confidential data;
- Access to personal confidential data should be on a strict need-to-know basis;
- Everyone with access to personal confidential data should be aware of their responsibilities;
- Comply with the law; and
- The duty to share information can be as important as the duty to protect patient confidentiality.

4.3 Duty of Confidentiality

A duty of confidentiality is owed to all individuals who provide information to you in confidence. This information may only be disclosed for the purposes that the subject knows about and has consented to unless there is a legal requirement for disclosure.

All staff members should be familiar with this common law duty and also the Confidentiality: NHS Code of Conduct 2003. Guidance is also published by healthcare professional bodies. Principle 5 of the Code published by the Nursing and Midwifery Council confirms that all nursing practitioners owe a duty of confidentiality to all those receiving care. Other healthcare professions have similar guidelines affirming a practitioner's duty of confidentiality.

See Section B for further information on the Trust's obligations to keep information confidential and how it handles personal data.

4.4 National Data Security Standards

The National Data Security standards were compiled following the WannaCry cyber security incident which affected a large number of NHS systems. The standards are the Government's required standards which all public sector organisations must meet, as follows:

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

8. No unsupported operating systems, software or internet browsers are used within the IT estate.

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

4.5 Legislation, Regulations and Guidance

In addition to the specific legislation and guidance set out above, the Trust must also consider other legal and professional requirements when dealing with personal data, as set out in Section 7 below.

The Trust, as a data controller, has responsibility for ensuring that all of these principles are met. The Trust is meeting this responsibility by enacting this and the subordinate policies.

5 Duties and Responsibilities

5.1 Chief Executive Officer

The Chief Executive has overall responsibility for data security and protection within the Trust, with responsibility for the implementation delegated to the Director of Corporate Governance.

5.2 Caldicott Guardian

The Medical Director of the Trust is also the Trust's Caldicott Guardian. The Caldicott Guardian will ensure the organisation implements the Caldicott Principles and Data Security Standards with respect to confidential patient data. They will oversee the arrangements for the use and sharing of clinical information and provide advice on lawful and ethical use of such information.

5.3 Senior Information Risk Owner ("SIRO")

The SIRO is accountable for information risk within the Trust and to provide written advice to the Accounting Officer on the content of the Trust's Statement of Internal Control in regard to information risk.

The SIRO's key responsibilities are:

- understand how the strategic business goals of the Trust may be impacted by information risks and how those risks may be managed;
- oversee the development of an information risk policy and monitor its appropriateness;
- be compliant with NHS data security and protection policy, standards and methods;
- act as an advocate for information risk on the Board;
- take ownership of the assessment processes for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control;
- ensure that the Board are adequately briefed on information risks issues;
- review and agree actions in respect in respect of identified information risks to provide assurance that information risks have been appropriately assessed and counter measures put in place;
- ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff; and
- undertake information risk management training at least annually to be able to demonstrate their skills and capabilities are up to date and relevant to the needs of the Trust.

Operational responsibility for information security shall be delegated by the SIRO to the Information Security Specialist (ISS). All information security risks shall be managed in accordance with the Risk Management Policy.

5.4 Data Protection Officer ("DPO") / Head of Information Governance

The DPO is responsible for ensuring that the Trust and its constituent business areas remain compliant at all times with the relevant legislation, regulations and guidance. The DPO reports directly to the Board and Chief Executive, and shall:

- inform and advise the Trust on all issues regarding its data protection obligations;
- monitor compliance with the GDPR;
- lead on the provision of expert advice to the organisation on all matters concerning the DPA 2018, compliance, best practice and setting and maintaining standards;
- provide a central point of contact for the DPA 2018 both internally and with external stakeholders (including the Office of the Information Commissioner);
- communicate and promote awareness of the GDPR and DPA 2018 across the Trust; and
- lead on matters concerning individuals' rights to access information held by the Trust and the transparency agenda

The DPO also has responsibility for the completion, accuracy and submission of the Data Security and Protection Toolkit ("DSPT") annual return.

The DPO is also Head of Information Governance in the Trust. The Head of Information Governance is responsible for co-ordination of and management of information governance and information governance policies across the Trust and ensuring policies are in place for the protection of staff, patient and sensitive organisational information.

The Head of Information Governance is also responsible for and for the secure and authorised access / use of the Electronic Patient Record Systems. They also investigate any unauthorised access to electronic patient records and undertake data protection impact assessments.

The Head of Information Governance exercises these functions on a day to day operational basis via the Deputy Head of Information Governance.

5.5 Information Security Specialist

The Information Security Specialist is responsible for ensuring that all personal identifiable information is processed and stored securely and is responsible for implementing, monitoring, documenting and communicating security requirements for the organisation. The Information Security Manager is responsible for leading the identification, delivery and management of an Information Risk management programme to address and manage risks to the Trust's information assets and maintains the Information Asset Register.

The Information Security Manager is also responsible for the monitoring of all incidents relating to information governance, which includes incidents involving paper records or documents containing person identifiable information.

The Information Security Specialist will keep the Information Governance Steering Group informed of the information security status of the organisation by means of bi monthly reports to the Information Governance Steering Group.

5.6 Information Asset Owners ("IAO")

Information Asset Owners are accountable to the SIRO for providing assurance that information risk is being managed effectively, for the information assets of which they have been assigned ownership. Each of the Directorates / Divisions will have an IAO who will be at Senior Management level, with the duties of compiling the details of the information assets delegated to leads within their respective areas of responsibility.

Information Asset Owners need to understand and are responsible for:

- identifying and documenting all Information Assets they own;
- taking ownership of their local asset control, risk assessment and management processes for the information assets they own;
- providing support to the SIRO to maintain their awareness of the risks to all Information Assets they own;
- knowing what information the assets hold and who has access to the information assets and why, and ensure their use is monitored and compliant with information governance standards of good practice and Trust policies and procedures;
- ensuring that all information flows and transfers are identified and mapped. Also, that all such flows and information transfers are approved, legitimate, secure and minimised but sufficient to achieve and support business and service needs and purposes;
- ensuring business continuity arrangements and contractual service arrangements are in place and up to date for the information assets;
- approving and overseeing the disposal mechanisms and arrangements for information of the asset when no longer required;
- ensuring that staff and other relevant users are aware of and comply with expected data security and protection working practices for the effective use of owned Information Assets;
- providing a focal point for the resolution and/or discussion of risk issues affecting their information assets;
- ensuring that the Trust's requirements for information incident identification, reporting, management and response apply to the Information Assets they own via the Trust's Incident Management and Reporting Policy;
- fostering an effective data security and protection culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the Trust's policy; and nominating and appointing Information Asset Administrators.

5.7 Line Managers

Line Managers are responsible for ensuring that all staff are fully aware of this policy and their individual responsibilities for the handling of information they have access to within their roles. This includes being responsible for their staff's supervisory records.

Managers must ensure that all staff receive and attend adequate training to comply with information governance requirements and apply the appropriate policies and procedures.

Managers must ensure that this policy and associated standards will be incorporated into local processes and updated as necessary in the event of any changes to national or local standards. Assurance will be provided to the Information Governance Steering Group that any changes identified have been implemented.

5.8 Staff (including students on placement)

All staff must be aware of this and all subordinate policies and ensure they have completed annual data security and protection mandatory training and any other related Information Governance training that is relevant to their role.

All staff must be vigilant with regards to malicious software, spam emails alongside social engineering attempts, such as being asked for your password and or log in details, and should follow the trust IT and incident reporting processes.

Every member of staff is responsible for the records they create, hold, use and/or share and must ensure appropriate levels of security are applied.

All staff must ensure that any incidents relating to breaches of codes of practice, policies, procedures and legal requirements and / or professional codes of ethics are reported appropriately and in a timely manner in line with the Trust incident reporting process and policy. [link to other policies]

As well as being required to understand and implement the contents of this policy, each staff member will have signed up to binding clauses relating to confidentiality and data protection with the Trust as part of their contracts of employment. All agency and Bank staff will also be expected to comply with the terms of this policy and all other Trust policies relating to Data Security and protection.

5.9 Third Parties

Contracts with external contractors and organisations that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all the Trust's information security policies, as set out at Chapter 8 below. Where contracts are not being issued, third parties must be required to sign a confidentiality agreement and statement.

5.10 Committees

5.10.1 Digital Transformation Executive

This committee receives, on request, reports on the progress of the DSPT submission and information governance work plan.

5.10.2 Information Governance Steering Group

This Group is responsible for co-ordinating information governance in the Trust. The group develops and maintains data security and protection policies, standards, procedures and guidance and oversees the annual submission of the DSPT. The group will ensure that all areas of Information Governance are adequately represented by the appropriate subgroups to ensure effective delivery of DSPT requirements and compliance with associated standards and legislation. This group is responsible for the approval of this policy.

6. Definitions

6.1 Duty of confidence

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is generally accepted that information provided by patients or service users to a health care service is confidential and must be treated as such so long as it remains capable of identifying the individual it relates to. Once the information is effectively anonymised it is no longer confidential.

6.2 Personal information (also known as person identifiable information)

Personal information is information about a living individual who can be identified from that information and other information the data controller (i.e. the Trust) holds or is likely to hold in the future. The Trust holds personal identifiable information about its patients about Trust staff and Trust members. Personal information may include but is not limited to:

- name, address, postcode, telephone number, date of birth, gender, ethnicity
- occupation & salary details
- National Insurance number, staff number, NHS number or other local identifier such as hospital or GP practice number
- photographs, videos, audio-tapes, images of patients, staff and members
- anything else that may be used to identify a patient, staff or a member directly or indirectly such as rare diseases or drug treatments

No personal information that is given or received in confidence may be passed to any other individual without the knowledge or consent of the person providing the information except in the circumstances set out in Section 12.

6.3 Personal confidential data / information

Personal confidential data / information is personal information about identified or identifiable individuals which should be kept private or secret. This is information that is provided on the understanding and assumption that it will not be disclosed to any other individual without prior consent of the provider of the information. There are some exemptions to this rule, such as if there is a law or court order which states information must be disclosed or if disclosure is considered to be in the public interest.

Confidential information can be found in a variety of media such as paper, hard disk, diskette, tape, radiology images, video, photographs, electronic records, and can also be given verbally.

6.4 Sensitive personal information

Sensitive personal information is identified in the Data Protection Act as a specific category of personal information which is of a sensitive nature. For this type of information even more stringent measures should be employed to ensure that the data remains secure. Sensitive personal information contains details of a person's:

- physical or mental health or conditions
- sexual life
- biometric data
- racial or ethnic origin
- religious beliefs or other beliefs of a similar nature
- trade union membership
- political opinions
- commission or alleged commission of any offence
- any proceedings, disposal or sentence given for the commission or alleged commission of any offence

6.5 Pseudonymisation

Pseudonymisation occurs when patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.

6.6 Anonymisation

Anonymisation occurs when information does not identify an individual directly and which cannot reasonably be used to determine identity. Information can be used more freely if the subject of the information is not identifiable in any way. When anonymised information will serve the purpose, health professionals must anonymise information. Whilst it is not necessary to seek patient consent to use this type of information, general information about when anonymised data will be used should be made available to patients.

6.7 Data controller

Data controller is the term given in the Data Protection Act for the person or organisation who decides the purposes for which data is or will be processed. The Trust is the data controller for its patient, staff and member information.

6.8 Data processor

Data processor is the term given in the Data Protection Act for the organisation or person (other than the data controller's staff) who is processing data on behalf of the data controller. Appropriate confidentiality and data protection clauses need to be in place in contracts, to ensure that data processors manage personal information in accordance with the Trust's policies and procedures.

6.9 Data subject

Data subject is the term given in the Data Protection Act for the person who is the subject of personal data. Patients, staff and members of the Trust are data subjects.

6.10 Explicit consent

Explicit consent is an articulated agreement by an individual; it is a clear and voluntary indication of preference or choice, usually given orally, in writing or by another form of communication such as signing and freely given in circumstances where the available options and the consequences have been made clear. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health care.

6.11 Implied consent

Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed.

6.12 Data breach

A data breach may occur when personal information is disclosed, changed in some way or mislaid or is no longer available, in circumstances where the data subject would have a reasonable expectation that the information concerned ought to have been secured and preserved. Any incident concerning a breach of personal data should be reported via the Trust's incident reporting system in line with the Trust's Incident Management and Reporting policy.

7. Procedures/Process

How the Trust Should Handle Personal Data

7.1 Guidance and Principles

All staff must ensure that the following principles are adhered to:-

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your Line Manager or the Information Governance Team.

The Trust is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever appropriate, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice. For advice and further guidance on Subject Access requests, please see the Trust's Access to Records Procedure.

7.1.1 Office Environment

Access to rooms and offices where terminals are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked. No personally identifiable information should be left out on desks. Computer screens should be locked when staff are away from their desks and any smart cards removed from smart card terminals. Any smart cards left in terminals when any staff member is absent from their desk will be removed and confiscated and should be passed securely to the IG team.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

The Trust's Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

7.1.2 Disclosing Personal/Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Office Anonymisation Code of Practice (https://ico.org.uk/).

- When the information is required by law or under a court order. In this situation staff must raise in the first place with the IG team by emailing the IG team inbox – bchc.informationgovernance@nhs.net. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority. Referred to as approval under s251 of the NHS Act 2006.

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must raise in the first place with the IG team by emailing the IG team inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must raise in the first place with the IG team by emailing the IG team inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

If staff have any concerns about disclosing information they must raise in the first place with the IG team by emailing the IG team inbox. The IG team will then consult the DPO or Caldicott Guardian if necessary before advising.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. Data sharing agreements provide a way to formalise arrangements between organisations. For further information on Data Sharing Agreements contact the IG team by emailing the IG inbox.

Staff must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data. When legitimately

transferring patient information or other confidential information by email, services or methods that meet NHS Encryption standards must be used. Emails between NHS Mail accounts meet this requirement (nhs.net to nhs.net). Emails between NHS Mail and other secure government domains also meet this requirement (e.g. nhs.net to gsi.gov.uk). As there are a number of these, please consult the Corporate IG team for advice when intending to send confidential information by email to a non-nhs.net address.

It is not permitted to include confidential or sensitive information in the body of an email. When e-mailing the information must be sent as an encrypted attachment with a strong password communicated through a different channel or agreed in advance.

Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent or the information is not person-identifiable or confidential information.

7.1.3 Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry Trust information (or any confidential information) with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

Taking home/ removing paper documents that contain person-identifiable or confidential information from Trust premises is discouraged. Staff must minimise the amount of person-identifiable information that is taken away from Trust premises. To ensure safety of confidential information staff must keep them on their person at all times and in a locked bag whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times, kept out of sight whilst being transported and kept in lockable locations and should not be left overnight anywhere in a car or other vehicle.

When working away from Trust locations staff must ensure that their working practice complies with the Trust's policies and procedures. Any electronic removable media must be encrypted as per the current Trust policy regarding removable media. Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately-owned computer or device.

If staff need to carry person-identifiable or confidential information or take such information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Any memory sticks in use by a member of staff must be encrypted. It is a disciplinary offence for any member of staff to use an unencrypted memory stick for any Trust business, whether or not the memory stick contains personally identifiable information. Any staff member requiring a memory stick should raise a request with the IT helpdesk, confirming why the request is being made and for what purpose.

7.1.4 Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally or allow it to become mislaid or lost. Staff may be held personally liable for a breach of the requirements set out in this policy and this may lead to disciplinary action and potentially dismissal. In particular staff must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard;
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents;
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended. Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers. Any patient identifiable information held in paper format must be kept in a locked bag when removed from Trust premises secured using combination locks provided by the Trust. Should staff require any combination locks please contact the IG team by emailing the IG team inbox;
- Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

7.1.5 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted (e.g. viewing your ESR record). Under no circumstances should employees access records about their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018 and may be reported to the ICO for criminal prosecution. When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the Trust. If staff have concerns about this issue they should discuss it with their Line Manager, Information Governance Team or DPO.

7.1.6 Filming / recording staff and patients & media enquiries

Individuals (who are not considered to be data controllers) such as patients can process personal data such as photographs they may take whilst in hospital if they use it only for 'domestic purposes'.

The use of cameras and mobile phones with cameras (or other similar devices with cameras) in private areas (for example, bathrooms, toilets, secluded areas) or other clinical areas may not however, sufficiently ensure medical confidentiality or protect a patient's or staff member's right to respect for their private life. The Trust therefore prohibits the use of such devices to take unauthorised photographs or video footage by either staff or patients where there is no clear clinical need to do so or where suitable prior consent has not been obtained. If staff identify any individual who may have taken photo or video images on a media device or phone this should be immediately escalated to their team leader who should raise a Datix incident and inform the Legal Services department immediately who will provide further advice. The team leader should address this issue with the identified person who may have taken the images and ask to see any images taken. If any images are identified on that individual's phone which have been obtained without any clear consent, the individual should be asked to delete them from their device immediately. If they refuse, Legal Services should be informed and further advice sought.

Patients or their family and friends can record staff who enter the patient's home using a mobile phone, digital camera or CCTV, with or without the staff member's knowledge or consent if the information is for their own domestic use. However, sharing or disclosing the recording without the consent of the member of staff may go beyond domestic purposes and therefore be subject to the provisions of Data Protection legislation. If the staff member becomes aware that the recording has been disclosed outside of the patient's home they should notify their line manager and report this as an incident. Depending on the nature of the disclosure, further action may then be taken by the Trust.

Any requests by external organisations to film on Trust premises must be made in writing to the Corporate Affairs and Legal Services Manager and the Communications Team. If an external organisation wishes to use patient or staff images in any film or photograph taken on Trust premises their explicit consent must first be sought and the consent must also be recorded. Patients and staff should be issued with a privacy notice to ensure they understand the uses their personal information may be subject to. Patients and staff have the right to refuse to be filmed and this right must be respected.

Any requests from members of the press or other media communications for information relating to the Trust, its staff or patients must be passed immediately to the Communications Team and the Legal Services team. No member of staff should release, discuss or disclose information of any kind to the media without permission. Any member of staff who does so may be subject to disciplinary action.

7.2 Data subjects' rights

In order to ensure compliance with the data subjects rights, prior to their data being processed, data subjects should be informed about:

- the identity of the data controller(s);
- the purpose(s) of the processing;
- any disclosures to third parties that are envisaged; and
- an indication of the period for which personal data will be kept.

If the purpose for processing data changes, the ROPA will be updated and the data subject will be informed.

The lawful basis for processing personal data has an effect on the data subjects' rights. For instance, if the Trust relies on someone's consent to process their data, then they will generally have stronger rights to have their data deleted.

7.2.1 Right to be informed

The Trust will provide 'fair processing information', typically through a privacy notice published on the Trust's website, which provides transparency about how the Trust collects and uses personal data. The information the Trust supplies in the privacy notice must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child;
- Available in a format suitable for people with learning disabilities or with impaired vision; and
- Free of charge.

In addition to the privacy notice being available on the Trust's website, if the Trust obtains the personal data directly from a data subject it must supply the privacy notice at the time that the data is collected.

In addition to the privacy notice being available on the Trust's website, if the Trust obtains the personal data from another source it must provide the data subject with the privacy notice within a reasonable period of having obtained the personal data (typically, within one month), or if the Trust is using the personal data to communicate with the data subject, at the latest, when the first communication takes place. The Trust does not need to provide information if to do so would require a disproportionate effort.

The Trust's privacy notice can be found at:

http://www.bhamcommunity.nhs.uk/about-us/corporate-information/privacy-notices-and-data-protection/

7.2.2 Right to access and alter the data or the way in which it is managed

Data subjects have a right to make a request to access information the Trust holds in relation to them and also to dictate how this data is managed. All requests by data subjects should be managed in accordance with the Subject Access Request policy.

7.3 Record of Processing

Compliance with the data protection principles

In order to ensure compliance with the data protection principles, all staff and personnel working for, or on behalf of the Trust, including agency staff and contractors, will:

- record directly or notify the Information Governance manager to record the lawful condition, the purposes for processing of the personal data in the ROPA and the date by which such information should no longer be held by the Trust (notwithstanding any legal obligation to retain the personal data);
- ensure that all personal data collected is sufficient to allow the Trust to provide the relevant service to the data subject but that no unnecessary information is held. If data is provided or obtained which is excessive for the purpose, it will be immediately deleted or destroyed. If data is provided that is no longer relevant for the purpose, it should be managed in accordance with the Records Management Policy;
- ensure the accuracy of data obtained either directly from the data subject or via a third party. If the data subject informs the Trust of a (factual) inaccuracy and the Trust agrees, the data will be amended to reflect this as soon as practicably possible. Exceptionally a note will be appended to the record to indicate that the data subject does not agree that the data held is accurate;
- retain information in accordance with the Trust's retention schedule set out within the Records Management Policy;
- ensure all information relating to patients and staff is kept secure at all times by managing it in accordance with the:

    - Data Security and Protection Policy;
    - Email Policy;
    - Internet Policy; and
    - Records Management Policy.

The Record of Processing Activity (RoPA) can be found at http://nww.bhamcommunity.nhs.uk/about-us/divisions-and-directorates/finance-directorate/information-governance/ig-information-asset-register/. The Information Governance manager has responsibility for maintaining the ROPA.

Failure to ensure that all processing of personal data is reflected within the Trust's ROPA constitutes an offence under the GDPR and Data Protection Act 2018.

The ROPA is reviewed and updated on a regular basis or whenever a new type of processing takes place. It is available to the ICO upon request.

7.4 Maintaining compliance with data protection obligations

The Trust will review all the relevant policies, procedures, contracts and agreements annually and conduct regular information audits as part of its obligations under the annual DSP toolkit submission, to ensure its data protection obligations set out in this policy continue to be met.

Any complaints about the Trust's Data Protection procedures and management of data should be directed to the Data Protection Officer, who will deal with the complaint in accordance with the Trust's Complaints Policy.

General enquiries about the GDPR or Data Protection Act should be directed to the Information Governance Manager who will provide advice to the relevant department of the Trust in support of the resolution of the enquiry

This policy is not a stand-alone document and should be read in conjunction with the policies, procedures and strategies set out elsewhere in this document.

8. Information Security

8.1 Introduction

Information Security is about people's behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology.

The aim of the Trust's Information Security policy is to preserve:

(i) Confidentiality – access to data shall be confined to those with appropriate authority

(ii) Integrity – information shall be complete and accurate. All systems, assets and networks shall operate correctly and according to specification

(iii) Availability – information shall be available and delivered to the right person, at the time when it is needed.

The Trust needs to ensure that Trust systems are in place and enabled so as to adequately protect its assets from both internal and external vulnerabilities.

8.2 Legal background – Network Information Systems (NIS) Regulations 2018 and GDPR

The NIS Regulations were implemented at the same time as GDPR (25 May 2018). The NIS regulations apply to "operators of essential services", eg public utilities, NHS Trusts, and any private companies operating essential public services. The Regulations are intended to ensure that such organisations have appropriate measures in place to protect them from cyber security attacks and that they are being actively monitored and implemented. Compliance with the DSP toolkit will enable a Trust to validate that they are compliant with the NIS Regulations.

8.3 Policy framework

I. Security Control Assets and risk assessments

The Trust will develop and implement an asset management system to control and manage its data and information flows across the Trust and to clearly identify how and with whom personal data is being shared. All ICT assets will have a named Information Asset Owner who shall be responsible for the information security of that asset. IAOs shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

II. Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO.

III. Computer Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

IV. Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

V. Equipment Security

In order to minimise loss of, or damage to, all assets, the Corporate Ditigal Technology Services (DTS) Team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

VI. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of the Trust.

VII. Information Security Events and Weaknesses

All Trust information security events, near misses, and suspected weaknesses are to be reported to the Head of Corporate ICT Technology & and Security or designated deputy and where appropriate reported as an Adverse Incident. All adverse incidents shall be reported to the Trust DPO. The Information Security Incident Reporting procedures must be complied with.

VIII. Protection from Malicious Software

The organisation and its DTS providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the DTS Head of Technical Services. Users breaching this requirement may be subject to disciplinary action.

IX. Removable Media

Staff must not use removable media to transmit data to and from Trust systems unless that media has received appropriate encryption. Users breaching this requirement may be subject to disciplinary action.

X. Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The Trust will put in place routines to regularly audit compliance with this

and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

XI. Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements).
Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

XII. IG requirements for New Processes, Services, Information Systems and Assets

The IG requirements for "Privacy by Design and Default" policy must be complied with when:

- A new process is to be established that involves processing of personal data (data relating to individuals)
- Changes are to be made to an existing process that involves the processing of personal data;
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data.
- Introducing any new technology that uses or processes personal data in any way.

XIII Accreditation of Information Systems

The organisation will ensure that all new information systems, applications and networks include a security plan and are approved by the SIRO and Caldicott Guardian before they commence operation and that a data protection impact assessment has been completed.

All Trust systems will also be required to adhere to Clinical Safety Standards (https://digital.nhs.uk/clinical-safety/clinical-risk-management-standards); The following

two standards, relating to clinical safety, are accepted for publication under section 250 of the Health and Social Care Act 2012 by the Standardisation Committee for Care Information (SCCI). SCCI0129 – This standard sets clinical risk management requirements for Manufacturers of health IT systems. SCCI0160 – This standard requires a health organisation to establish a framework within which the clinical risks associated with the deployment and implementation of a new or modified health IT system are properly managed. Appropriate assessments will be undertaken by the Trust Clinical Safety Officer as part of any system development/implementation.

9. National Opt-Out Framework

The national data opt-out applies to the disclosure of confidential patient information for purposes beyond individual care across the health and adult social care system in England. The national data opt-out applies to data that originates within the health and adult social care system in England and is applied by health and care organisations that subsequently process this data for purposes beyond individual care. This may be data that is used to

- Plan services by understanding what services patients may be using and why;
- Predict what services will be required in the future and what level of resourcing and financing is necessary;
- look at diseases and illnesses and their treatments to see whether anything unexpected is happening, such as whether patients on certain medications are at a higher risk of developing other conditions, like heart disease or stroke;
- identify the risk factors for disease and its severity, such as age, gender, ethnicity, where patients live, or another health problem, like high blood pressure or obesity;
- monitor the outcomes of a new drug or type of treatment to see if it is effective or whether it has side effects.

The national data opt-out choice

The national data opt-out allows a patient to choose that they do not want their confidential patient information to be used for purposes beyond their individual care and treatment. All health and care organisations in England are required to apply the national data opt-out by March 2020. A patient can change their mind and update their national data opt-out choice at any time. A patient can choose to opt out but still agree to take part in a specific research project or clinical trial.

The opt-out applies regardless of the format and includes structured and unstructured electronic data and paper records. When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed. The NHS number is used as the identifier for the removal of the records.

A patient's national data opt-out will not apply where data is legally required to be shared, or if there is an overriding public interest. The national data opt-out will not prevent anonymised data from being used for purposes beyond individual care, where it is anonymised in line with the Information Commissioner's Office code of practice on anonymisation. In addition, the national data opt-out is for patient data only and applies to confidential patient information - the national data opt-out does not apply to workforce or staff data. NB: Staff data may be removed as a result of the opt-out being applied but only where it is relevant to a patient's care (for example, a consultant's name may be linked to an episode of care). Staff data, and any other personal data which is not confidential patient information, would still be subject to data protection legislation and the rights provided under this, including article 21 (right to object) in GDPR, but sits outside of the scope of the national data opt-out**.**

Organisations completing the DSP Toolkit are asked to confirm that they maintain a record (e.g. register or registers) that details each use or disclosure of personal information including the legal basis for the processing and, if applicable, whether national data opt-outs have been applied.

The national data opt-out will apply when:

(i) Confidential patient information is used for purposes beyond an individual's care and treatment, AND
(ii) The legal basis to use the data is approval under regulation 2 or 5 of the Control of Patient Information Regulations 2002, section 251 of the NHS Act 2006.

In general, where section 251 NHS Act 2006 is being relied upon as the lawful basis (under the Common Law Duty of Confidentiality) to process confidential patient information then the national data opt-out will apply.

Confidential patient information

Confidential patient information is defined in section 251(11) of the National Health Service Act 2006. Broadly, it is information that meets the following three requirements:

- Identifiable, or likely identifiable (e.g. from other data in possession of the recipient),
- Given in circumstances where the individual is owed a duty of confidence; and
- Conveys some information about the physical or mental health or condition of an individual

It cannot be defined in terms of specific data items but by considering the circumstances of the disclosure. For example, with demographic information (like name and address): Demographic data from a registration record, e.g. Personal Demographics Service (PDS), is personal data, but not confidential patient information as it does not contain information about the physical or mental health or condition of an individual. Demographic data along with any clinical data, or from a medical record, is confidential patient information.

Who does the national data opt-out apply to?

All health and care organisations that act as a sole data controller or a joint data controller for patient data have a responsibility to consider the national data opt-out policy and ensure it is being applied in accordance with the policy and in line with the wider implementation timetable. The Trust also has a responsibility to ensure that any data processors acting on its behalf are also applying the national data opt-out.
Application of the national data opt-out

NHS Digital has developed the service and systems to enable patients to set, view and change their national data opt-out choice. National data opt-outs are stored centrally in a separate opt-out repository on the NHS Spine, against the patients' NHS numbers. NHS Digital are the data controller for patients' national opt-out data and have responsibility for ensuring that all national data opt-outs recorded by patients, and any changes to a patient's national data opt-out, are processed accurately and recorded in the opt-out repository on the NHS Spine.

Trust staff are informed that, at the time of writing, the Trust is working with NHS Digital to implement a solution whereby the Trust is informed of any data sharing restrictions placed on a patient's record for purposes beyond their individual care. This policy will be updated to take account of any developments in this area going forward.

10. Implementation

Following ratification the procedural document's author/lead will ensure (in discussion with the Committee's Secretary) that the document is forwarded to the Quality and Standards Assurance Team (Q&SAT). The Q&SAT will make final checks, amend the footer and forward to the Library for uploading to the intranet. Once uploaded to the intranet the Library will inform the Communication Team to ensure notification appears in the next Staff E-Newsletter**.**

In addition this policy will be circulated to all Executive Directors, Associate Directors, Divisional Directors and published on the Intranet site by the information governance manager. It will be circulated to Divisional Leads, Heads of Service and Service Managers / Leads for wider dissemination.

The awareness of this policy will be supported by the information contained on the information governance intranet pages.

11. Duty of Candour

The Trust recognises it has a duty of candour under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 20. Under this duty it has a responsibility to be open and transparent with patients, families and carers in relation to their care and treatment and has specific requirements when things go wrong. This will include informing people about any clinical incident, providing reasonable support, providing truthful information and an apology when things go wrong. If an incident occurs which involve a breach of the requirements of this policy, staff and managers should consider following the guidance set out in the Being Open incorporating Duty of Candour Policy available on the trust intranet site.

12. Implications

12.1 Training Implications

Information Security is covered within the Trust's Information Governance mandatory training and all new staff will receive Information Governance awareness training at induction which also includes elements of Information Security.

Ad-hoc advice and guidance will be available from the Information Governance team and intranet pages.

An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

12.2 Financial Implications

The implementation of this policy requires no additional financial resource.

12.3 Legal Implications

Any serious breaches of GDPR and Data Protection Act 2018, caused by failing to comply with this policy, could result in fines being imposed on the Trust by the Information Commissioners Office up to a maximum of €20,000,000 or 4% of turnover, whichever is the greater.

13. Monitoring & Audit

The Information Governance Steering Group (IGSG) receives reports which include Information Governance Incidents, Mandatory Training compliance and the Information Governance Work plan on a bi-monthly basis.

Element to be monitored	**Lead**	**Tool**	**Frequency**	**Reporting arrangements**	**Acting on recommendations and Lead(s)**	**Change in practice and lessons to be shared**
What key element(s) need(s) monitoring as per local approved policy or guidance?	**Name the lead and what is the role of the multidisciplinary team or others if any.**	**What tool will be used to monitor/check/ observe/assess/ inspect/ authenticate that everything is working according to this key element from the approved policy? This could be an audit, or risk assessment document**	**How often is the need to monitor each element? How often is the need complete a report? How often is the need to share the report?**	**Who or what committee will the completed report go to and how will this be monitored. How will each report be interrogated to identify the required actions and how thoroughly should this be documented in e.g. meeting minutes.**	**Which committee, department or lead will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations within reasonable timeframes?**	**How will system or practice changes be implemented and the lessons learned and how will these be shared?**
Information Assets	Deputy Head of Information Governance	Information Asset Register	Monitored monthly via service level reports and reviews	SIRO receives copies of the divisional annual reports	Information Security manager/ Divisional leads	Divisional leads to share via team meetings
Information Governance Incidents	Deputy Head of Information Governance	Datix extract and Local Database	Monitored daily, with reports produced bi monthly.	Information Governance Steering Group	Incident Handlers and Line managers	Information Governance Steering Group Team Meetings

Data Security and Protection Toolkit	Data Protection Officer	Data Security and Protection online submission	Annual submission	Information Governance Steering Group Quality Safety and Risk Committee	Information Governance Steering Group	Information Governance Steering Group
Information Governance Training Compliance	Deputy Head of Information Governance/ Learning and Development	Learning & Development Reports Online Information Governance Training Tool	Bi Monthly	Information Governance Steering Group	Line managers / HR when training trajectories are not met	Information Governance Steering Group

14 References/Evidences/Glossary/Definitions

- Common Law Duty of Confidentiality
- Data Protection Act 2018
- General Data Protection Regulation 2016
- Network and Information Systems Regulations 2018
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Human Rights Act 1998
- Data Security and Protection Toolkit - NHS Digital
- ISO/IEC 27001 Information Security Management Standard
- NHS Code of Practice: Confidentiality 2003
- NHS Code of Practice: Records Management 2016
- Regulation of Investigatory Powers Act 2000