Family Nursing & Home Care

Information Governance Policy and Procedures

4 May 2022

Document Profile

Document Registration	Added following ratification
Type	Policy
Title	Information Governance Policy and Procedures
Author	Claire Whelan Head of Information Governance and Systems, with support from Mo de Gruchy Quality and Performance Development Nurse
Category	Information Governance
Description	Information Governance Policy and Procedures
Approval Route	Organisational Governance Approval Group
Approved by	Rosemarie Finley
Date approved	4 May 2022
Review date	3 years from approval
Document Status	This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Version control / changes made

Date	Version	Summary of changes made	Author
March 2022	1	This is a new policy which combines and supersedes the previous individual policies for Data Protection, Confidentiality and Information Security. Layout and wording has been revised – States of Jersey is now Government of Jersey Content updated in line with revised Data Protection (Jersey) Law 2018	Claire Whelan/ Mo de Gruchy
March 2022	1.1	Updated to also incorporate FNHC Email Policy, Records Management Policy, Subject Access Request Policy and Retention Schedule	Claire Whelan/ Mo de Gruchy

CONTENTS

1. INTRODUCTION

1.1 Rationale

Information is integral to delivering good health care. Most staff deal with information on a daily basis to effectively carry out their duties and therefore confidentiality and good data control are extremely important in all areas.

The lawful and correct treatment of person-identifiable information by Family Nursing & Home Care (FNHC) is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. All staff have a common law duty of confidence and breaches of confidentiality can adversely affect the organisation's reputation and credibility.

FNHC has a legal obligation to comply with all appropriate legislation in respect of Data, Information and Information Technology (IT) Security. Penalties could be imposed upon the organisation and its employees as well as adversely affecting its reputation and credibility for non-compliance with relevant legislation.

This policy is intended to inform staff of the structure of the Data Protection (Jersey) Law 2018 and other relevant legislation and recommendations and their personal responsibilities in relation to the use of confidential information. This will help FNHC ensure that all person-identifiable information is handled and processed lawfully and correctly.

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

1.2 Scope

This policy applies to all FNHC Trustees, Committee members and staff on permanent, temporary or voluntary contracts, including those co-located to work on behalf of FNHC, who have access to personal identifiable information, whether written, computerised, visual, audio or held in the memory of a member of staff.

1.3 Role and Responsibilities

FNHC Trustees

FNHC Trustees, collectively known as the 'Data Controller', permit the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The FNHC Committee members have legal responsibility for the notification process and compliance with the Data Protection (Jersey) Law 2018.

Chief Executive Officer

The CEO has overall accountability for the management of information governance within FNHC.

Director of Governance, Regulation and Care

The Director of Governance, Regulation and Care has a particular responsibility for ensuring that FNHC corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Senior Information Risk Officer (SIRO)

The Senior Information Risk Owner: The SIRO is FNHC's CEO and has overall responsibility for the organisation's Information Risk Management. The SIRO also leads and implements the IG risk assessment and advises the Trustees Board on the effectiveness of IRM across the organisation.

Head of Quality, Governance & Care

The Head of Quality, Governance & Care is the Caldicott Guardian and is responsible for the overall development and maintenance of information governance within FNHC, in particular for drawing up guidance for good practice and promoting compliance with this policy.

Head of Information Governance and Systems

They are responsible for ensuring a fit for purpose and ratified policy is in place and for ensuring that the procedures and controls required in support of this policy are developed and maintained. They are responsible for managing associated risks and escalating to the appropriate person where necessary. They also act as the organisation's Data Protection Officer (DPO).

Caldicott Guardian

FNHC's Caldicott Guardian has a particular responsibility for protecting the confidentiality of people's healthcare data. They are responsible for ensuring it is shared in an appropriate and secure manner.

Line Managers

All the managers across the organisation's business units are directly responsible for:

- Ensuring their staff are made aware of this policy and any notices
- Ensuring their staff are aware of their data protection responsibilities
- Ensuring their staff receive suitable data protection training
- Monitoring compliance to the requirements of the data protection policy within their team

All Staff

All FNHC employees, including temporary and contract staff and those co-located to work on behalf of FNHC, are subject to compliance with the policy. Under the Data Protection (Jersey) Law 2018 individuals can be held personally liable for data protection breaches. Staff must attend mandatory training in Information Governance annually.

2. POLICY

This overarching Information Governance policy provides an overview of the organisation's approach to information governance and includes data protection and other related information governance policies and details about the roles and management responsible for data security and protection in the organisation.

Information, whether in paper or digital form, is the lifeblood of FNHC because of its critical importance to patient care and other related business processes. High-quality information underpins the delivery of high-quality evidence based healthcare and many other key service deliverables.

FNHC information may be needed to:

- support patient care and continuity of care;
- support day-to-day business processes that underpin the delivery of care;
- support evidence-based clinical practice;
- support public health promotion and communicate emergency guidance;
- support sound administrative and managerial decision making, as part of the knowledge base for the organisation;
- meet legal requirements, including requests from patients under the provisions of the Data Protection Law
- assist clinical or other types of audit;
- support improvements in clinical effectiveness through research

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. With the increasing reliance on IT and the transmission of information across networks or computers, it is necessary to ensure that FNHC ensures their systems are developed, operated, used and maintained in a safe and secure way.

Information has greatest value when it is accurate, up to date and is accessible where and when it is needed. Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue mission critical processes, and these factors should be fully considered when commissioning, designing or implementing new systems. An effective information security management regime, therefore, ensures that information is properly protected It is essential that personal information be effectively protected against improper disclosure at all times.

2.1 Key Principles

FNHC obtains and processes person identifiable information for a variety of different purposes, including but not limited to:

- Staff records and administrative records
- Delivery of Health Care
- Fundraising

Such information may be kept in either computer or manual records. FNHC needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Person-identifiable information is defined as 'information which relates to an individual and from which they can be identified, either directly and indirectly'.

Person-identifiable information at FNHC can include employees (present, past and prospective), patients/service users, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

2.2 Legal Considerations

There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. Legal requirements and permissions are continually being added to; further information is available from the DPO. Generally, however, the main areas of law, which constrain the use and disclosure of personal information, are briefly described below.

2.2.1 Data Protection Law and principles

Irrespective of how the information is collected, recorded and processed, person-identifiable information must be dealt with properly to ensure compliance with the Data Protection (Jersey) Law (DPJL) 2018. This Law requires FNHC to comply with the six Data Protection (DP) Principles and to notify the Information Commissioner about the data that FNHC holds and why FNHC holds it. This is a formal notification and is renewed annually.

This Law also gives rights to data subjects (people that FNHC hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask FNHC to stop using it and to seek damages where FNHC are using it improperly.

The DP Principles are as follows:

- ✓ Data is processed lawfully, fairly and in a transparent manner in relation to individuals

- ✓ Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

- ✓ Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- ✓ Data is accurate and where necessary kept up to date, every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

- ✓ Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

- ✓ Data is processed securely and against accident loss, destruction or damage by using appropriate technical or organisational measures

Under the DP legislation Personal Data is defined as:

"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

Special Categories of Personal Data is defined as:

"Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

Information Governance also enables the organisation to ensure that all confidential information is dealt with legally, securely and efficiently, in order to deliver the best possible care to its patients.

<u>Data Subjects Rights</u>

Data Subjects also have rights under the new legislation:

1. The Right to be Informed
2. The Right of Access
3. The Right to Rectification
4. The Right to Erasure.
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights in relation to automated decision making and profiling

Subject Access Requests

A Subject Access Request (SAR) provides a right for the data subject/applicant to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, where it is reasonable to do so.

Information must be supplied to the data subject/applicant in an intelligible, easy to understand form, unless to do so would involve 'disproportionate' effort. For manual records this would involve photocopies. For computerised records these can be supplied in electronic format but must contain explanations of codes or abbreviations where appropriate. If the 'disproportionate' effort issue arises, the records can be shared with the individual on a face to face basis, who can be asked to visit the premises to view their records. All Subject Access Requests should be forward without delay to the DPO.

Any information that constitutes personal data or special categories of personal data of the subject/applicant should be provided (subject to any data protection exemptions or information that may cause harm or distress).

Under the DPJL and the General Data Protection Regulations (GDPR) FNHC is required to respond to a valid subject access request without undue delay and in any event within four weeks of receipt of the request from the data subject. The period may be extended by a further eight weeks where necessary, taking into account the complexity and number of the requests.

In the case of further extension, the DPO will inform the data subject of any such extension within four weeks of receipt of the request, together with the reasons for the delay. Failure to do so is a breach of the Legislation and could lead to a complaint being made to the Jersey Office of the Information Commissioner (JOIC).

To assist the obligation to provide information within the time limits, FNHC will ensure that all staff are aware of the SAR process and the requirements to provide the information when requested by the DPO.

SARs will be acknowledged by FNHC within 2 working days after the date of receipt of the request. Letter templates are held with the DPO.

Where FNHC requires clarification of a request the four week rule is suspended until the clarification is received. i.e. Invalid ID

Where required, FNHC will endeavor to provide advice in respect to complex request. This may include:

- If the request is unclear and further clarification is needed;
- If the information has been requested in a particular unacceptable acceptable or unreadable format;
- Where complying with the request would involve disclosure of personal data about another individuals;

- If the information requested is subject to one or more of the exemptions in the Data Protection Legislations.

Requests for personal information and communication provided under the GDPR shall be provided free of charge. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character FNHC may either:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- Refuse to act on the request

FNHC will ensure the balance of probability and fairness have been carefully considered when demonstrating the manifestly unfounded or excessive character of the request.

Where personal information is being requested by a representative (e.g. solicitor/advocate) of the data subject, FNHC must be satisfied that the representative has the authority to make the request on behalf of the data subject and that the appropriate authorisation to act on their behalf has been included.

Where FNHC cannot comply with a request without disclosing information relating to other individuals who can be identified from that information, FNHC is not obliged to comply with the request unless:

a) the other individual has consented to the disclosure of the information to the person making the request, or
b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual, for example, redacting (blanking out) the name or other identifying features

FNHC will provide the data subjects/applicants with information that constitutes their personal information only, and will ensure that a duty of confidentiality owed to the other individual (s) is respected.

Where a representative/solicitor is making a SAR on behalf of an adult who lacks capacity to consent to the SAR, the DPO or staff dealing with the request must be satisfied that the request has been made in the individual's best interest. This may include requesting approval from the data subject's legal guardian or medical practitioner.

A registered health professional may believe that providing an individual with access to certain information might cause serious harm to their physical or mental health or to that of another person. If so, the Capacity and Self Determination (Jersey) Law 2016 allows FNHC (as the data controller) to withhold the information. However, only a health professional can make such a decision, and it must be fully documented.

This exemption does not apply to information that the individual already knows.

If an individual disputes some of the information held within their record this should be discussed with the DPO.

There are various grounds where personal data does not have to be provided, in part or in full. These include:

- ✓ Where complying with the request would involve disclosure of personal data about other individuals who have not given their consent, and redacting (blanking out) their personal information or other identifying features is impossible
- ✓ Where disclosure would be likely to prejudice an ongoing enquiry or investigation. Where this can be demonstrated, FNHC does not need to disclose the existence of such information
- ✓ If the information requested is subject to one or more of the exemptions in the DP Legislations
- ✓ Where it is a repeated or similar request and FNHC had previously complied with the request, unless a reasonable interval has elapsed
- ✓ If providing documents would involve disproportionate effort* or expense. If this is the case the data subject must be informed what information is held, the source of the information, the purpose it is being processed and who it may be disclosed to. This 'exemption' would usually only apply to situations where there is a very large amount of data held within an unstructured (paper) filing system

*The term 'disproportionate effort' refers to the time and cost of complying with a request and this must be balanced against the effects on the individual requesting the information of not supplying the information. In FNHC this situation should seldom arise.

The DPJL and GDPR give certain provisions which allow public authorities to withhold information from an applicant where an exemption applies. Therefore, in some cases, there will be valid reasons why some information may not be released to an applicant and these include:

- ➢ If the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings
- ➢ If the disclosure of personal data to third parties contravenes the first data protection principle (process fairly and lawfully)

It is important to note that if an exemption is applied under DP Legislations the DPO or the member of FNHC staff applying the exemption should be aware that they may need to substantiate their decision if challenged by the applicant or the JOIC as part of the review process. It is therefore advisable to document decisions (including legal basis) made in relation to using exemption or redaction.

In all cases where an exemption is cited (and a refusal notice issued) the balance of factors for and against should be explained to the applicant in the reply.

In some circumstances FNHC may be legally required to share personal information with law enforcement and regulatory bodies (without the consent of the data subject). The legal basis and justification for the sharing may be underpinned by the following Articles of the DPLJ:

- Article 64 - Permitted processing for law enforcement, legal proceedings and public records purposes;
- Article 65 - Exemptions by Regulations.

FNHC will review each request based on its merits before deciding whether to release information to the 'relevant authorities'.

Subject Access Request

Data Protection Impact Assessments

In line with the guidance from the JOIC, a Data Protection Impact Assessment (DPIA) must be undertaken for any project, procurement, business case and transfer of personal data or departmental/team initiative where there is a potential impact upon the privacy of individuals.

A DPIAs is a risk assessment tool used to analyse how a particular project or system will affect the privacy of the individuals involved. The JOIC uses the term 'project' in a broad and flexible way – it means any plan or proposal in an organisation and does not need to meet an organisation's formal or technical definition of a project, such as set out in a project management methodology. This includes potentially any proposal, procurement, business case and/or departmental/team initiative that includes transfers of personal data and/or potential sensitive business information.

The DPIA process must be integral to conventional project management techniques and be started from the very earliest stages of the project's initiation, often as a result of the business case process being invoked.

As DPIAs are chiefly concerned with an individual's ability to manage their information; FNHC's processes are therefore aligned to DP and Caldicott Principles (also see 2.2.4), with specific concentration being given to the minimising of harm arising from intrusion into privacy, as defined by those principles.

An effective DPIA allows FNHC to identify and resolve any such problems at an early stage, minimising costs and reputational damage which might otherwise occur.

2.2.2 Common Law Duty of Confidentiality

The legal obligation for confidentiality is one of common (case) law, rather than statutory law, which means it will change as case law evolves. Essentially it means that when someone shares personal information in confidence it must not be disclosed without some form of legal authority or justification. In practice this will often mean that

the information cannot be disclosed without that person's explicit consent unless there is another valid legal basis (UKCGC 2021).

2.2.3 Jersey Care Commission requirements

As a registered care provider in Jersey FNHC is required to adhere to the Jersey Care Commission Care Standards for Home Care. Standard 2.7 states that "Information held on record will be up to date and necessary and will be kept confidentially. Information about people who receive care will only be shared with those who have a legitimate need to know the information. People who receive care will understand who will have access to their information, what information is shared and why" (JCC 2019).

2.2.4 The Caldicott Report & Principles

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

The Caldicott Principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information.

Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian.

<u>Principle 1: Justify the purpose(s) for using confidential information</u>

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

<u>Principle 2: Use confidential information only when it is necessary</u>

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

2.2.5 Freedom of Information

Family Nursing & Home Care (FNHC) are not a Scheduled Public Authority for the purposes of the Freedom of Information (Jersey) Law 2011 (the “FOI Law”) and therefore do not have an obligation to respond to an FOI request.

This is because, whilst the definition of ‘public authority’ in Article 1 of the FOI Law is broad enough to include FNHC the duties and obligations of the FOI Law only apply

to those entities listed in Schedule 1 to the Law, known as Scheduled Public Authorities. This list is limited and FNHC are not specifically listed.

It is possible that we may be asked to provide information to a Scheduled Public Authority like the Health and Community Services Department, in order to assist with an FOI request they are dealing with, but there is no obligation to provide this information unless the information held by FNHC was held 'on behalf' of the Scheduled Public Authority (i.e. not exclusively held for FNHC purposes).

Any FOI requests must be forward to the DPO.

2.3 Duty of Confidentiality

Respect for confidentiality is an essential requirement for the preservation of trust between patients and health care professionals. Without assurances about confidentiality, patients may be reluctant to provide the information that is needed to deliver appropriate levels of care.

Health Care Professionals hold information about patients that is private and sensitive. This information is collected to provide care and treatment to individuals and generally must not be used for other purposes without the individual's knowledge and consent.

Confidentiality should only be breached in exceptional circumstances and with appropriate justification. When a health care professional can justify that information should be released they should act promptly to disclose all relevant information. This is often essential to the best interests of the patient, or to safeguarding the well-being of others. Any such breaches should be fully documented giving justification for the breach.

The organisation holds personal information about each staff member and this information must be treated with the same level of confidentiality with which patient information is held.

2.4 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.

The obligation to confidentiality is:

- ✓ A duty under common law
- ✓ A requirement established within professional codes of conduct
- ✓ Included within employment contracts as a specific requirement linked to disciplinary procedures

Patients entrust FNHC with, or FNHC to gather, sensitive information relating to their health and other matters as part of their seeking treatment and advice. They do so in confidence and they have the legitimate expectation that staff will respect their privacy

and act appropriately. It is essential that personal information be effectively protected against improper disclosure at all times.

Patient Identifiable Information includes the following:

Surname	Forename
Initials	Address
Date of Birth	Other key dates eg death, diagnosis
Postcode	Occupation
Sex	Unique Reference Number (EMIS)
Ethnic Group	Telephone Numbers

Examples of transferring personal identifiable information include:

- ✓ Taking a document and giving it to a colleague
- ✓ Making a telephone call/having a conversation
- ✓ Sending a fax
- ✓ Sending an email
- ✓ Passing information held on computer

In some circumstances patients may lack the capacity to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of the patients is to be retained, that FNHC provides, and is seen to provide, a confidential service.

Information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, fully anonymised information is not confidential and may be used with care.

It is extremely important that patients are made aware of information sharing that must take place in order to provide them with high quality care. Whilst patients may understand that information needs to be shared between healthcare professionals they may not be aware of sharing between different organisations involved in the provision of their healthcare. Efforts must be made to inform them of everyone who will be sharing their information.

Equally, clinical governance and clinical audits, which are wholly proper components of health care provision, might not be obvious to patients and use of information in this way should be drawn to their attention.

Patients should be informed about:

- ✓ The use and disclosure of the information associated with their healthcare
- ✓ The choices that they have and the implications of choosing to limit how information may be used or shared

Patients/clients generally have the right to object to the use and disclosure of their confidential information and need to be made aware of their right. Patients need to be

made aware that by not consenting to certain disclosures they may be compromising their care. Clinicians cannot usually treat patients/clients safely, nor provide continuity of care, without having relevant information about a person's condition and medical history.

All staff should ensure that no personal data is disclosed either verbally or in writing, to any unauthorised third party. Staff must not assume that work colleagues are authorised to see the same information as they are. If staff are in doubt as to whether they should share the information with one of their colleagues, they must seek the advice of their manager in the first instance.

2.5 Records Management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through the lifecycle to eventual disposal.

The Records Management: NHS Code of Practice© has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice and FNHC will follow these guidelines.

FNHC's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of FNHC and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

FNHC is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- ✓ better use of physical and server space
- ✓ better use of staff time
- ✓ improved control of valuable information resources
- ✓ compliance with legislation and standards
- ✓ reduced costs

FNHC also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

The following relates to all clinical and non-clinical operational records held in any format by FNHC. These include:

- all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints)

- all patient health records (for all specialties including clinical photographs, imaging reports and photographs

The importance of sound records management practices:

- Records management is most effective when it is regarded as a professional activity requiring specific expertise

- Records are a valuable resource because of the information they contain. That information is only useable if it is correctly and legibly recorded in the first place, is regularly updated, and is easily accessible when it is needed

The aim of the FNHC Records Management System is to ensure that:

- records are always available when needed - from which FNHC is able to form a reconstruction of activities or events that have taken place

- records can be accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist

- records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records

- records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated
- records can be maintained through time – the qualities of availability, accessibility, interpretation and FNHC worthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format

- records are secure - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required

- records are retained and disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value

- staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management. Training should be evidenced and measured through audits.

2.5.1 Inventory of records

FNHC will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The inventory of record collections will facilitate:

- ✓ the classification of records into series
- ✓ the recording of the responsibility of individuals creating records

The register will be reviewed annually.

2.5.2 Storage, Tracking and Transportation of Records

Records must always be kept securely but a balance needs to be achieved between security and accessibility. The following must be considered when deciding upon suitable storage and the physical location of keeping records.

- ✓ Security levels required/risk assessment
- ✓ Compliance with Health & Safety regulations
- ✓ User needs
- ✓ Record types
- ✓ Size and quantity
- ✓ Usage and frequency of retrieval
- ✓ Suitability of space and price
- ✓ Retention periods
- ✓ Legislation

All staff are responsible for the safe custody of records in their use. Personal identifiable information must be handled in accordance with the Data Protection Jersey Law 2018.

All documentation should be stored in an appropriate filing system, whether physical and electronic. It is acknowledged that individual departments may have different record filing systems, however, the principles of good filing should be adhered to by all staff. Filing documentation is the responsibility of the individual who last made an entry in the record.

Under no circumstances should personal identifiable information be left out in the open e.g. on a desk or on a computer screen when staff are not at their desk for prolonged periods of time and especially of an evening when information should be locked away securely, adhering to a Clear Desk Policy, or in any place visible to the public e.g. when in the car. Where rooms containing unsecured records are left unattended, they must be locked.

Records should be stored securely in either a locked cabinet or within a secure environment on a computerised system.

If records are being delivered to another location they should be enclosed in envelopes and sealed for transfer.

For larger quantities, records should be boxed in suitable boxes, mail bags or containers for their protection. Each envelope or box should be addressed clearly and marked confidential.

Any records containing personal information which is carried to/from departments these must be done so in an envelope/mail bag.

If working from home patient/client records should not be taken home to carry out duties unless in exceptional circumstances and this should be discussed with the Operational Lead and DPO to carry out a risk assessment.

Vehicles containing records should never be left unlocked when unattended and records must be kept out of view.

2.5.3 Tracking

Record tracking is the process of recording the movement of a record to produce an audit trail (a list of the record's movements). This enables the record to be located and retrieved quickly and efficiently at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transaction.

It is essential that appropriate staff are aware of the location of the records in their charge, that those records are accessible whenever required and are retained according to FNHC's Record Retention Schedule.

To ensure that records are not misplaced or lost, each department must ensure that it has a system for tracking and tracing records, which is maintained by all staff.

Tracking systems should include the following information:

- ✓ The item reference number or other identifier
- ✓ Brief description of item
- ✓ Name of the person to whom the record is being sent, their department and contact number
- ✓ Date of transfer
- ✓ Expected date of return
- ✓ Name of the person recording the movement
- ✓ Any special instructions on return if necessary

2.5.4 Missing Records

If a record cannot be found the Data Protection Officer must be informed immediately. When all efforts to find the record have been exhausted, an Information Security Incident should be logged on ASSURE Incident Reporting System.

2.6 Retention and Disposal of Records

It is a fundamental requirement that all of FNHC's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time

for retaining records will depend on the type of record and its importance to FNHC's business functions. See Appendix 1

2.6.1 Archiving Records

Office space is at a premium and it is rarely possible to retain all records created in offices, therefore 'inactive' records should be sent to the Data Protection Officer for archiving.

FNHC has an archiving stores based at Gervaise Le Gros and Le Bas Centre. This is where information is stored that has to be retained for a specified purpose.

Any staff member wishing to archive information must:

- ✓ Ascertain what they require to keep
- ✓ Put the information into an envelope if only a small amount or for larger amounts archiving boxes provided ensuring that they are not too heavy
- ✓ Print off an archiving box form from central files and complete the relevant details requested
- ✓ Give the box to the DPO who will ensure that it is stored in the relevant area within the Store for the required retention period

2.6.2 Destroying Records

In order to protect itself and minimise risk of breach of the Data Protection Law, FNHC should not maintain records for longer than necessary, nor should they destroy records sooner than is required.

FNHC's Records Retention Schedule (Appendix 1) details the types of information held by the Organisation and how long it has be retained for.

The following types of non-health records are also covered by the retention schedule:

- Personnel Records
- Financial and Accounting Records
- Corporate records
- Records associated with complaint handling
- Photographs
- Emails

Once the retention period has been reached, hard copy confidential records must be destroyed in securely in the shredding bins provided.

2.6.3 Destruction of Health Records

Records should not be destroyed before the end of the relevant period shown.

A log of health records destroyed and the date of destruction will be kept electronically by the Data Protection Officer or Medical Records and Archiving Clerk.

Destruction must ensure confidentiality and the shredding bins provided must be used.

2.7 Staff Contract Of Employment

The FNHC Staff 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.

All temporary staff, volunteers and students are required to sign a Confidentiality Statement Form (Appendix 2)

2.8 FNHC Committee Members

All confidential information heard, created or accumulated by the Committee must be used on a strict need to know basis, and must not be disclosed to anyone other than persons authorised to receive it, both during their term in office as a Committee Member and beyond it. All Committee members will be required to sign a Confidentiality Agreement (Appendix 3).

FNHC Committee Members must ensure that:

- ✓ confidential manual records are kept as securely as possible -if information is no longer required, it can be taken to the Association to be destroyed securely
- ✓ the Association email address, issued through the Government of Jersey network, is used for all Association business purposes and contacts
- ✓ the Association's computer device is securely password protected
- ✓ all Association related documents are saved to the GOJ 'L' Drive' in the following folder: \\hss\fnhc\Committee
- ✓ they check their email address regularly, at the very minimum twice a week, to avoid missing vital information
- ✓ when using the Association's laptop, they must comply with all the Government of Jersey Specific Information Security Procedures which the Association abides by.
- ✓ every effort is made to ensure that the Association laptop does not get misplaced, lost or stolen - in the unlikely event of this happening they contact the Association's Head of Information Governance & Systems immediately
- ✓ when leaving the post of Committee Member, their laptop and any information relating to the Association whether, electronic or paper is returned to the Head of Information Governance & Systems to be dealt with appropriately

2.9 Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information.

2.9.1 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 license from the supplier.

2.9.2 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.

2.10 Equipment Security

In order to minimise loss of, or damage to, all assets, Head of Information Governance & Systems shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards. All adverse incidents shall be reported to the Head of Information Governance & Systems. FNHC's Incident Reporting procedures must be complied with.

2.11 Protection from Malicious Software

The organisation will work together with GoJ IT service providers to ensure software countermeasures and management procedures are in place 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 GoJ IT Dept. Users breaching this requirement may be subject to disciplinary action.

2.12 Monitoring System Access and Use

An audit of system access and staff data use shall be maintained and reviewed on a regular basis. FNHC 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.

2.13 System Change Control

Changes to information systems, applications shall be reviewed and approved by the Head of Information Governance & Systems and the GoJ IT Department if necessary.

2.14 Business Continuity and Disaster Recovery Plans

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.

2.15 IG Requirements for New Processes, Services, Information Systems and Assets

The IG requirements for New Processes, Services, Information Systems and Assets procedure 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

2.16 Inappropriate Use of Information Systems

It is not acceptable for staff to access records on computer systems on behalf of themselves, relatives, friends or neighbours. There are proper channels for accessing the information. Staff must not access patient or staff information for anything other than their official duties, as misuse of the computer system may result in disciplinary action.

2.17 Security Incidents

A security incident is anything that happens to any type of information that should not occur, e.g. breach of confidentiality, breach of security.

A security incident is an event that may result in:

- Degraded system integrity
- Loss of system availability
- Disclosure of confidential information
- Disruption of activity
- Financial loss
- Legal action
- Unauthorised access to applications

Breaches of security can include:

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of removable storage devices e.g. memory sticks due to an individual's carelessness
- Accessing a computer using someone else's password either fraudulently or by accident
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building

Breaches of confidentiality can include:

- Finding a computer printout with header and personal information on it at a location outside of FNHC
- Paper or electronic records about a patient/member of staff or business information found at a location outside FNHC
- Being able to view patient records in the back or front of an employee's car
- An email being received by the incorrect recipient
- Giving information to people who are not entitled to know either verbally, written or electronically

All security incidents must be reported using the organisation's incident reporting system ASSURE as soon as it is realised that it has happened, as per the FNHC Incident Reporting SOPs. Certain types of personal data breach also need to be reported to the JOIC. This must be done without undue delay, within 72 hours of becoming aware of the breach, not after investigation. The DPO should review all reported data breaches and notify the JOIC where this is required.

To prevent such incidents recurring and where appropriate, staff will be made aware of incidents that have occurred, issues identified and any changes in process.

2.18 Training

All staff will receive training in information governance and security as part of their Induction and will also be required to complete mandatory updates.

3. PROCEDURES

3.1 Password Management

Passwords shall be used to ensure that access to systems, devices and information is controlled and restricted to approved and authorized users only.

Passwords shall be complex in nature

Unique passwords shall be created and used by individuals for each system to which they require access.

3.1.1 Standard User Account Access Government of Jersey (GoJ)

- ✓ Minimum length 15 characters
- ✓ Cannot be the same as any of the previous 5 passwords
- ✓ Any characters can be used
- ✓ No change period required (Change can be carried out by end users or administrator
- ✓ Password must be changed when the account is first used
- ✓ Password cannot be consecutive sequence of letters/numbers, eg. abcde or 123456
- ✓ Password cannot contain a month, season year or numbers that can be interpreted as dates
- ✓ Password cannot contact the user name

3.1.2 Other Systems

As a best practice guide, passwords should be created in the following format:

- ✓ A minimum of 8 characters long
- ✓ Contain at least two uppercase letters
- ✓ Contact at least two lower case letters
- ✓ Contain at least 2 numbers
- ✓ Contain a least two special characters or non-alphanumeric characters such as £%$!@

3.1.3 Password Security

All passwords shall be protected to the same level as that afforded to the system or information that they provide access to.

Users shall ensure that passwords are not shared with other users. (If there is a business requirement to share a password approval shall be obtained from the Management).

Users shall ensure that passwords are never revealed to any other persons. This includes system administrators, security staff and management.

All Local Server Administrator passwords should be changed every 90 days.

If there is any indication that a password has been compromised that password shall be changed immediately and reported as a security incident.

An organization's passwords are the 'keys' to its systems, data and information. Adequate protection must be provided to all passwords and thereby the assets they protect, in order to prevent their loss, compromise or use by unauthorized

3.2 Secure Working Area

Identification badges are issued to staff and should be worn at all times. Temporary staff shall be issued with a badge for the duration of their employment.

All visitors and trades people must report to Reception where they must sign the Visitors book and wear a visitor badge. All visitors will be supervised while on the premises and staff informed where practical.

Staff should ensure that upon leaving the building their computers are shut down and all equipment attached, e.g. printers turned off, drawers and cabinets are locked, lights switched off and all windows and doors are closed. Fire doors shall be kept closed at all times.

All desks should be left tidy and all confidential paperwork locked way.

3.3 Room Access and Transporting Records

Records should be stored securely in either a locked cabinet or within a secure environment on a computerised system.

All staff should ensure that they transport records securely (see FNHC Record Keeping Policy).

3.4 Conversations

Staff must ensure they cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings and when they have information discussions with colleagues about confidential information.

Do not identify a patient or staff member by name unless it is safe to do so.

If personal identifiers are necessary, please remember the following:

- Consideration needs to be given to the position of any answer phone to ensure that recorded conversations cannot be overheard or otherwise inappropriately accessed
- In clinical areas staff should be aware that other patients in the same room/clinic area might overhear them. Whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patients' right to confidentiality
- It is not appropriate to discuss personal information in public areas e.g. corridors, stairways, staff kitchen areas
- When speaking to a patient, carer or staff member on the telephone, confirm the caller's identity and ensure they are entitled to the information they are requesting. If in any doubt about the identity of the caller, take their telephone number, verify it independently and call them back
- If a phone is left unattended during a call ensure the hold/mute button on the telephone is activated
- Identifiable information should not be used in training, testing systems, or demonstrations without explicit consent. Test data should be used for this purpose
- If in doubt, always ask

3.5 Safeguarding Computerised Information

The security and confidentiality of information held on computer must be maintained at all times. Any electronic information relating to patients, i.e. letters, emails should be printed off and kept within the patients' record either paper or electronic.

Never leave a computer logged on to a system and unprotected. Always protect the system by pressing Control, Alt & Delete simultaneously on your keyboard and select the option "lock computer”. This applies no matter how long you are leaving your computer unattended.

Always log off when you have finished. This prevents the risk of unauthorised access to patient information. It also ends the user's session on the computer. Turn off the computer at the end of the working day. If it is necessary to leave it switched on for technical reasons, make sure it is locked using Control, Alt & Delete plus option "lock computer'.

Never store personal identifiable information on the 'H Drive'. Seek guidance from the Head of Information Governance and Systems.

Passwords protect both the information and the user. Passwords must never be disclosed to anyone else under any circumstances.

Never use anyone else's password or login.

3.6 Email Management

Email enables FNHC employees to communicate promptly and efficiently with other employees, individuals and organisations, as part of their employed roles.

Email can also generate risks to the organisation, especially where employees use it outside of their employed role.

The following rules are to be strictly adhered to:

- ✓ Do not send or forward emails containing any material that is offensive, pornographic or obscene, which damages someone’s reputation, or which is meant to annoy, harass or intimidate another person in any way
- ✓ Do not send emails that contain jokes, gossip, rumours or suggestive or insulting remarks that could lead to misunderstanding, hurt feelings or legal claims
- ✓ Do not forward a confidential message without acquiring permission from the sender first
- ✓ Do not forge or attempt to forge email messages
- ✓ Do not send email messages using another person’s email account
- ✓ Do not breach copyright or licensing laws when composing or forwarding e-mails and email attachments

3.6.1 Personal Use of Email

Reasonable personal use is permitted within the organisation provided it is consistent with the organisations standards and does not interfere with the performance of your duties.

Rules to follow regarding personal use:

- ✓ Make sure your emails do not interfere with your own or other email users' work, or other responsibilities.
- ✓ Do not send or deliberately receive offensive material.
- ✓ Do not use the email system for unlawful activities or to make money.
- ✓ Limit the personal emails you send. Do not send emails to other email users if it is not necessary.
- ✓ Avoid sending emails with large attachments. These can interfere with how the email systems or other computing facilities work, and may increase costs.
- ✓ Clearly identify all personal emails as personal in the subject line, this will ensure that the IT Department can respect your privacy.
- ✓ Do not use emails to send details of personal 'for sale' or 'wanted' items.

3.6.2 Acceptable Email Use

FNHC considers email as an important means of communication and recognises the importance of proper email content and speedy replies conveying a professional image and delivering a good service. Staff must therefore ensure they adhere to the following guidelines:

- ✓ Before sending an email, consider whether there is a more appropriate way of communicating e.g. telephone call or face to face contact
- ✓ Write well-structured emails and use short descriptive sentences
- ✓ Communicate only with those who are required to read the message
- ✓ Check that the emails are addressed to the correct recipient when using the Global Address Book
- ✓ Signatures must include employee's name, job title, organisation's name and address and contact number and website address
- ✓ Make sure that the standards for email content are the same as for letters, ensuring correct grammar and spelling and are professionally written
- ✓ Messages must be given a meaningful subject, do not leave subject lines blank, if an email is patient related the Unique Reference Number (URN) should ideally be in the subject heading if not then it must be clearly stated in the body of the email
- ✓ Communicate concisely and courteously, do not write in capitals as this appears as if one is shouting and is considered rude.
- ✓ Make sure emails are proofread carefully prior to sending
- ✓ Do not print emails unless this is really needed for work purposes. Emails can be saved if needed and should be kept for the period needed by law
- ✓ Observe email housekeeping rules, save emails in appropriate work areas and delete inappropriate and redundant material
- ✓ When forwarding emails, state clearly what action is expected from the recipient
- ✓ Emails should be treated like any other correspondence and should be responded to as quickly as possible
- ✓ Send requests for taking action to only one person where possible
- ✓ For messages that are sent to more than one person, clearly state who needs to take action
- ✓ Address those who need to be informed but do not have to take action or respond as 'cc', do not send to people unnecessarily

- ✓ When replying to an email, delete any unwanted addresses, use 'Reply to all' only when necessary – think carefully about whether everyone needs to see the response.
- ✓ A distribution list should only be used when the sender is sure that they need to send their message to everyone on the list and the message is relevant to the business
- ✓ If a reply to an email is needed by a particular date, let the recipient know this

3.6.3 Email Confidentiality

Every employee of FNHC is responsible for their emails and must comply with data protection legislation as well as their contract of employment.

Staff are responsible for making sure they do not send sensitive or confidential information by email internally, without the appropriate controls this includes taking extra care when selecting the address of the recipient, attaching the information as a Word document rather than straight on to the email. This includes information which is patient identifiable, employee information, organisation information.

All patient related emails should include a Unique Reference Number either in the subject heading or in the body of the email.

Staff should not send emails that contain sensitive patient information outside the organisation.

The Egress secure email system should be used to email documents which disclose personal information of a number of patients and clients, or hard copies should be sent via an alternative method such as post.

When exchanging important information by email, staff should contact the person sending it or receiving it, by another method of communication, to confirm their identity.

Staff must not send our intellectual property or sensitive information to people who are not authorised to see it, so remember to check email addresses carefully.

Remember emails can be forwarded to other email users without the original sender's knowledge. Avoid emails becoming lengthy and it is advisable to delete some of the information as new users could be included into the loop, who may not be authorised to see all the information.

The Government of Jersey IT Department have the right to see any email account at any time for any reason without giving staff notice, as long as they have received formal written approval from the Chief Internal Auditor and there are good reasons for doing so i.e. if they suspect a member of staff has broken their Information Security Policy.

3.6.4 Marking Messages

- ✓ Use the 'Urgent' flag only when absolutely necessary or it will no longer be effective

- ✓ Do not use the read receipt unnecessarily – it produces unnecessary emails particularly when it is used for emails sent to distribution lists. It should only be used when asking for important action and should normally be switched off
- ✓ Use the 'confidential' marker when the information is sensitive

3.6.5 Out of Office Reply

An 'Out of Office' reply must be set up when absent from the organisation for long periods of time. If you are absent due to sickness a Line Manager can arranged for an 'out of office' to be applied by the Service Desk.

3.6.6 'All User' Facility

Although email is often considered to be a good way of disseminating information to large groups, there are some restrictions. The ability to send an email to everyone within the organisation is restricted to designated staff.

Staff must not send 'all user' emails without permission. If staff feel they have a genuine business reason for doing this, they must discuss with their Line Manager.

Annual leave memorandums should only be sent to key staff members or immediate colleagues who are required to know.

If it is necessary to send an 'all user' email, staff must follow the good practice guidelines:

- ✓ Use corporate font – Arial 11
- ✓ All emails must have a title/heading
- ✓ Emails must have name, job title and extension number of sender at the end of the message
- ✓ Attachments should be kept to the minimum necessary and can be converted to PDF version to protect the content of the document and reduce the size if necessary
- ✓ Email users should not reply to the 'all user' email, if you wish to reply to a message use the forward button and enter the contact person

3.6.7 Housekeeping

It is the responsibility of all staff members to manage their email messages appropriately. It is important that email messages are managed in order to comply with the Data Protection (Jersey) Law 2018.

To manage email messages appropriately all staff must identify email messages that are records of the business activities. Clinical or managerial records should be moved within the mailbox and kept only for as long as required before being deleted.

A storage limit is sent on all email boxes. Staff will receive a warning message informing them when they are exceeding their limit and will not be able to send and receive emails until they have deleted or saved emails on the L: Drive.

Emails must be deleted on a regular basis, this includes inbox, sent items and deleted items.

4. CONSULTATION PROCESS

Name	Title	Date
Claire Whelan	Head of Information Governance and Systems	18/03/2022 25/03/2022
Elspeth Snowie	Clinical Effectiveness Facilitator	31/03/2022
Teri O'Connor	Home Care Manager	31/03/2022
Tia Hall	Operational Lead Adult Nursing	31/03/2022
Michelle Cumming	Operational Lead Child and Family Services	31/03/2022
Clare Stewart	Operational / Clinical Lead Out of Hospital Services	31/03/2022
Justine Le Bon Bell	Education Lead and Practice Development Nurse	31/03/2022

5. IMPLEMENTATION PLAN

Action	Responsible Person	Planned timeline
Email to all staff	Secretary/Administration Assistant (Quality and Governance Team)	
Policy to be placed on organisation's Procedural Document Library	Secretary/Administration Assistant (Quality and Governance Team)	

6. MONITORING COMPLIANCE

The Head of Information Governance and Systems will monitor compliance with this policy and procedures, using internal audit reviews where necessary, using the NHS Digital Data Security Standards. Line Managers should also monitor compliance within their service areas. Related incidents reported on Assure can be used as a learning resource.

7. EQUALITY IMPACT STATEMENT

Family Nursing & Home Care is committed to ensuring that, as far as is reasonably practicable, the way services are provided to the public and the way staff are treated

reflects their individual needs and does not discriminate against individuals or groups on any grounds.

This policy document forms part of a commitment to create a positive culture of respect for all individuals including staff, patients, their families and carers as well as community partners. The intention is to identify, remove or minimise discriminatory practice in the areas of race, disability, gender, sexual orientation, age and 'religion, belief, faith and spirituality' as well as to promote positive practice and value the diversity of all individuals and communities.

The Family Nursing & Home Care values underpin everything done in the name of the organisation. They are manifest in the behaviours employees display. The organisation is committed to promoting a culture founded on these values.

Always:

- ✓ Putting patients first
- ✓ Keeping people safe
- ✓ Have courage and commitment to do the right thing
- ✓ Be accountable, take responsibility and own your actions
- ✓ Listen actively
- ✓ Check for understanding when you communicate
- ✓ Be respectful and treat people with dignity
- ✓ Work as a team

This po0licy should be read and implemented with the Organisational Values in mind at all times.

8. GLOSSARY OF TERMS

Authorised Person - anyone who needs to know the Patient Identifiable Information to fulfil the responsibilities of their post

Patient Identifiable Information - items of information which relate to an attribute of an individual and potentially capable of identifying patients and hence should appropriately be protected to safeguard confidentiality

Personal Data - Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Data - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership**;** Genetic or biometric data that is processed for the purpose of uniquely identifying a natural person**;** Data concerning health**;** Data concerning a person's sex life or orientation**;** Data relating to a person's criminal record or alleged criminal activity

9. REFERENCES

Caldicott Committee (1997) *Report on the Review of Patient-Identifiable Information.* Department of Health, London

Jersey Care Commission (2019) *Jersey Care Commission Standards for Home Care.* Available at JCC-Care-Standards-Home-Care-2019-v1..pdf (carecommission.je). Last accessed 18th March 2022

Rotherham Doncaster and South Humber NHS Foundation Trust (2021) *Information Governance Policy and Management Framework (includes Data Protection Policy content).* Available at Information Governance Policy and Management Framework (includes Data Protection Policy content) – RDaSH NHS Foundation Trust. Last accessed 18th March 2022

States of Jersey (1995) *Computer Misuse (Jersey) Law (and 2019 amendments).* Available at CYBERCRIME (JERSEY) LAW 2019 (jerseylaw.je). Last accessed 25th March 2022.

States of Jersey (2005) *Regulation of Investigatory Powers (Jersey) Law*. Available at Regulation of Investigatory Powers (Jersey) Law 2005 (jerseylaw.je). Last accessed 25th March 2022.

States of Jersey (2011) *Freedom of Information (Jersey) Law.* Available at Freedom of Information (Jersey) Law 2011 (jerseylaw.je). Last accessed 25th March 2022.

States of Jersey (2018) *Data Protection (Jersey) Law.* Available at DATA PROTECTION (JERSEY) LAW 2018 (jerseylaw.je). Last accessed 18th March 2022

UK Caldicott Guardian Council (2021) *The Common Law Duty of Confidentiality.* Available at Duty of confidentiality — UKCGC. Last accessed 28th October 2021

10. APPENDIX

Appendix 1 FNHC Records Retention Schedule

Family Nursing & Home Care Retention Schedule

This is not an extensive list, and will be reviewed on a regular basis. If you require information on retention periods of something that is not listed, please seek advice from the Data Protection Officer

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
A & E computer print outs	Scanned on to patient record and destroyed	Destroy under confidential conditions
Children and Young People (all types of records relating to children and young people	Retain until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment or 8 years after death. If the illness or death could have potential relevance to adult conditions or have genetic implications the advice of clinicians should be sought as to whether to retain the records for a longer period	Destroy under confidential conditions
Counselling Records	30 years	Destroy under confidential conditions
Diaries - Office	1 year	Destroy under confidential conditions
Adult Services Records	8 years after conclusion of treatment or death	Destroy under confidential conditions
Health Records (excluding records not specified elsewhere in this schedule)	8 years after conclusion of treatment or death	Destroy under confidential conditions
Health Visitor Records	Records relating to children should be retained until their 26th birthday	Destroy under confidential conditions
Immunisation and Vaccination Records	Retain for the period of time appropriate to the patient	Destroy under confidential conditions
Photographs (Where the photograph refers to a particular patient it should be treated as part of the health record	Retain for the period of time appropriate to the patient	Destroy under confidential conditions

Refrigerator Temperature	1 year	Destroy
Scanned Records Relating to Patients	Retain for the period of time appropriate to the patient	Destroy under confidential conditions
Serious Untoward Incident Records	Permanent	
School Health Records (See Children and Young People)		
Video Records/Voice Recordings Relating to Patient Care/Video Conferencing Records	Retain for the period of time appropriate to the patient	

Business & Non-Health Records Retention Schedule

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Agendas of Board Meetings, Committees, sub-committees	Permanent	
Agendas	2 years	Destroy under confidential conditions
Audit Records (e.g. Organisational Audits, Records Audits, System Audits) internal and external and in any format i.e. paper/electronic	3 years from the date of completion of the audit.	Destroy under confidential conditions
Complaints – Correspondence, investigation and outcomes	8 years from completion to action	Destroy under confidential conditions
Abuse complaints relating to either staff or patients	25 years	Destroy under confidential conditions
Diaries - office	1 year after the end of the calendar year to which they refer.	Destroy under confidential conditions
Health & Safety Documentation	3 years	Destroy under confidential conditions
History of organisation	Permanent	
Incident Forms	10 years	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Records/documents relating to any form of litigation	Where a legal action has commenced, keep as advised by legal representatives.	
Manuals – Policy and procedures, administrative and clinical strategy documents	10 years after life of the system to which the policies and procedures refer	Destroy (policy documents may have archival value)
Meetings and minutes papers of major committees and sub-committees (master copies)	Permanent	
Meetings and minutes – other reference copies of major committees	2 years	Destroy under confidential conditions
Papers of minor or short lived importance not covered elsewhere e.g. • Advertising matter • Covering letters • Reminders • Letters making appointments • Anonymous letters • Drafts • Duplicates of documents known to be preserved elsewhere • Indices and registers complied for temporary purposes • Routine reports • Other documents that have ceased to be of value on settlement of the matter	2 years after the settlement of the matter to which they relate.	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Patient Surveys	2 years	Destroy under confidential terms
Phone message books	2 years, any clinical information should be transferred to the patient held record.	Destroy under confidential conditions
Press cuttings	Permanent	
Press Releases	7 years	
Project files	5 years	Destroy under confidential conditions
Public Consultations about future provision of services	5 years	Destroy under confidential conditions
Quality & Outcomes Framework	2 years	Destroy under confidential conditions
Receipts for Registered and Recorded Mail	2 years following the end of the financial year to which they relate	Destroy under confidential conditions
Reports (Major)	30 years	
Requests for access to records other than Subject Access Requests	6 years after last action	Destroy under confidential conditions
Statistics	3 years from date of submission	Destroy
Subject Access Request	3 years after last action	Destroy under confidential conditions
Time Sheets	6 months	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Buildings papers – relating to occupation of the building (but not health and safety information)	3 years after occupation ceases	Destroy under confidential conditions
Drawings – plans and buildings	Lifetime of the building to which they relate	
Equipment – records of non-fixed equipment, including specification, test records, maintenance records and logs	11 years	Destroy under confidential conditions
Inspection reports e.g. boilers, lifts	Lifetime of any installation	
Inventories of furniture, medical and surgical equipment not held on store charge and with a minimum life of 5 years.	Keep until next inventory	
Leases – the grant of leases, licences and other rights over property	Period of the lease plus 12 years	Destroy under confidential conditions
Maintenance contracts	6 years from end of contract	Destroy under confidential conditions
Manuals (operating)	Lifetime of equipment	Review if issues (egHSE) are outstanding
Medical Device Alerts	Retain until updated or withdrawn (check MHRA website)	Destroy under confidential conditions
Photographs of buildings	Lifetime of the building to which they relate	

Financial

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Accounts – annual (final – one set only)	Permanent	
Accounts – minor records (pass books, paying in slips, cheque counterfoils, cancelled discharged cheques, accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records)	3 years from completion of audit	Destroy under confidential conditions
Accounts – working papers	3 years from completion of audit	Destroy under confidential conditions
Advice notes (payments)	3 years	Destroy under confidential conditions
Audit records (internal and external audit) – original documents	10 years from completion of audit	Destroy under confidential conditions
Bank Paying in books	Current + 5 years	Destroy under confidential conditions
Bank Statements	3 years from completion of audit	Destroy under confidential conditions
Banks Automated Clearing System (BACS) Records	6 years after year end	Destroy under confidential conditions
Bills, Receipts and cleared cheques	6 years	Destroy under confidential conditions
Budgets (including working papers, reports and journals)	3 years from completion of audit	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Cash books	6 years after end of financial year to which they relate	Destroy under confidential conditions
Cash Sheets	6 years after end of financial year to which they relate.	Destroy under confidential conditions
Contracts – Financial	Approval files – 15 years Approved suppliers lists – 11 years	Destroy under confidential conditions
Contracts – non sealed (property) on termination	6 years after termination of contract	Destroy under confidential conditions
Contracts – sealed (and associated records)	Minimum of 15 years, after which they should be reviewed	Destroy under confidential conditions
Copy payrolls	5 Years	Destroy under confidential conditions
Cost accounts	3 years after end of financial year to which they relate	Destroy under confidential conditions
Creditor payments	3 years after end of financial year to which they relate	Destroy under confidential conditions
Debtor's records - cleared	6 years from completion of audit	Destroy under confidential conditions
Debtor's records - uncleared	6 years from completion of audit	Destroy under confidential conditions
Demand notes	6 years after the end of the financial year to which they relate	Destroy under confidential conditions
Expenditure sheets/books	10 years	Destroy under confidential conditions
Expense claims, including travel and subsistence claims, and claims and authorisations	3 years after end of financial year to which they relate	Destroy under confidential conditions

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Invoices	6 years after the end of financial year to which they relate	Destroy under confidential conditions
Ledgers, including cash books, income and expenditure journals, nominal rolls	6 years after end of financial year	Destroy under confidential conditions
Funding received by the organisation that does not directly relate to patient care e.g. charitable funds	6 years	Destroy under confidential conditions
Patient Monies (smaller sums of donated money)	6 years	Destroy under confidential conditions
Payments	6 years after year end	Destroy under confidential conditions
Payroll (i.e. list of staff in the pay of the organisation)	6 years after year end	Destroy under confidential conditions
Receipts	6 years after end of financial year to which they relate	Destroy under confidential conditions
Rents Receivable	10 years	Destroy under confidential conditions
Superannuation Accounts	10 years	Destroy under confidential conditions
Superannuation Registers	10 years	Destroy under confidential conditions
Tax Forms	6 years	Destroy under confidential conditions
Wages/salary Records	10 years after termination of employment	Destroy under confidential conditions

Purchasing/Supplies

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Purchase orders	3 years	Destroy under confidential conditions
Delivery Notes	2 years after end of financial year to which they relate	Destroy under confidential conditions
Goods received notes/dockets	3 years	Destroy under confidential conditions
Goods returned notes	3 years	Destroy under confidential conditions
Stock Control Reports	2 years	Destroy under confidential conditions
Stores Records – major (Ledgers)	6 years	Destroy under confidential conditions
Stores Records – minor (eg. Requisitions, issue notes, goods received books	2 years	Destroy under confidential conditions
Supplies records – minor (routine paper for requests for furniture, equipment, stationary and other supplies)	2 years	Destroy under confidential conditions

Personnel/Human Resources

TYPE OF RECORD	MINIMUM RETENTION PERIOD	FINAL ACTION
Criminal Record Bureau Disclosures	3 years	Destroy under confidential conditions
Disciplinary Documentation	Dependent on outcome of Action	Destroy under confidential conditions
Investigations	10 years	Destroy under confidential conditions
Job Advertisements	1 year	Destroy
Job Applications (Successful)	10 years following termination of employment	Destroy under confidential conditions
Job Applications (unsuccessful)	6 months	Destroy under confidential conditions
Job Descriptions	3 years	Destroy under confidential conditions
Letters of Appointment	10 years after employment has terminated	Destroy under confidential conditions
Personnel records	10 years after termination	
Pension Forms	10 years	Destroy under confidential conditions
Staff Car Parking Permits	3 years	Destroy under confidential conditions
Study Leave Application Forms	5 years	Destroy under confidential conditions
Timesheets for individual members of staff	3 years after which they relate	Destroy under confidential conditions
Training Plans	10 years	Destroy under confidential conditions

Appendix 2 Confidentiality Statement

Confidentiality Statement

Any information relating to the care or treatment of patients, and / or Association information or data is strictly private and confidential. The duty not to disclose any information to anyone outside the Association without authority, is a condition both during employment or placement with Family Nursing & Home Care and upon cessation of my employment/placement with Family Nursing & Home Care.

All Organisational procedures in relation to security systems must be complied with.

You will not on any occasion during or after termination discuss or disclose any information relating to your employment with any person outside the Association nor make any comments to the media either directly or through a third party which directly or indirectly adversely reflects on the Association and its standing in the community. Any such requests for information should be referred to the Chief Executive Officer.

I have read and understood the above conditions and agree to abide by the principles of confidentiality both during my employment I placement with Family Nursing & Home Care and upon cessation of my employment I placement with Family Nursing & Home Care.

Name: ……Signature:……

Date:……..

Witness:

Name:……Signature:……..

Date:.....

Appendix 3 Confidentiality Agreement for Committee Members

I (Name) ……
am aware of the relevant legislation, best practice guidelines and related Family Nursing & Home Care (Jersey) Inc. (the "Association") policies and procedures and agree that:

- I understand within the course of my work as Committee Member with the Association; I may have access to or hear confidential information about employees, patients or other business activities.

- I understand that no information of a confidential or personal nature concerning individuals or the Association may be disclosed without proper authority been given and that the information held by myself will be done so in a safe and secure manner. I confirm that information previously held on my personal devices prior to receiving an Association laptop has been transferred to the new device or deleted.

- I understand that following termination of my term in office with the Association that I will not discuss or disclose any information relating to the Association to anybody outside the Association nor make any comments to the media either directly or through a third party, which directly or indirectly adversely reflects the Association and its standing in the community.

PRINT NAME	
SIGNATURE	
DATE	
DESIGNATION	Chairman ☐ Vice Chairman ☐ Treasurer ☐ Committee Member ☐

On behalf of Family Nursing & Home Care (Jersey) Inc.

FNHC SENIOR MANAGER	
JOB TITLE	
SIGNATURE	
DATE	

Appendix 4 Equality Impact Screening Tool

Stage 1 - Screening			
Title of Procedural Document: Information Governance Policy and Procedures			
Date of Assessment	March 2022	Responsible Department	Governance
Name of person completing assessment	Claire Whelan	Job Title	Head of Information Governance and Systems

Does the policy/function affect one group less or more favourably than another on the basis of :	**Yes/No**	**Comments**
• Age	No	
• Disability Learning disability; physical disability; sensory impairment and/or mental health problems e.g. dementia	No	
• Ethnic Origin (including hard to reach groups)	No	
• Gender reassignment	No	
• Pregnancy or Maternity	No	
• Race	No	
• Sex	No	
• Religion and Belief	No	
• Sexual Orientation	No	
If the answer to all of the above questions is NO, the EIA is complete. If YES, a full impact assessment is required: go on to stage 2, page 2		

Stage 2 – Full Impact Assessment			
What is the impact	**Level of Impact**	**Mitigating Actions** (what needs to be done to minimise / remove the impact)	**Responsible Officer**

Monitoring of Actions
The monitoring of actions to mitigate any impact will be undertaken at the appropriate level