North East Lincolnshire

Information Governance Policy

Focus

Empowering individuals
to live independent lives

CONTENTS

1. INTRODUCTION

1.1 Information Governance Framework

This policy explains how Focus staff can manage and protect the information they use for their work, respecting the privacy and rights of service users and carers. The document also guides all Focus staff on Information Governance, which is a framework for handling personal information securely, ethically and professionally. Information Governance ensures that employees and others (such as contractors or agency staff) follow the same standards and rules when dealing with different types of information.

1.2 Policy Aims

The aims of this document are to maximise the value of organisational assets by ensuring that data is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully
- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.

Focus will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured.
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested.
- Information security training will be available to all staff
- All breaches of information security, actual or suspected, will be reported and investigated by the Head of Information Governance

2 ROLES AND RESPONSIBILITIES

2.1 Chief Executive / Caldicott Guardian

The Chief Executive has overall responsibility and is accountable to the board of Governors for all aspects of Information Governance in Focus and compliance with legislation and statutory guidance.

The Chief Executive will be the Focus Caldicott Guardian. They will:

- Ensure Focus satisfies the highest practical standards for handling personally identifiable information
- Facilitate and enable appropriate information sharing and make decisions on behalf of Focus following advice on options for lawful and ethical processing of information, in particular in relation to disclosure.
- Represent and champion information governance requirements and issues at Board level
- Facilitate and enable appropriate information sharing and make decisions on behalf of Focus following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies
- Co-ordinate the Information Governance Policy and its implementation

2.2 Senior Information Risk Officer (SIRO)

The SIRO will be responsible for:

- Acting as champion for information risk and advising the Board on the effectiveness of information risk management across Focus
- Promoting the effective and appropriate use of information
- Monitor Focus' information handling activities to ensure compliance with the law and guidance.

2.3 Data Protection Officer

The Data Protection Officer will be responsible for:

- Ensuring a yearly baseline assessment is undertaken using the NHS Data Security & Protection Toolkit (DSPT), along with the production and monitoring of action plans in relation to any gaps
- Ensure policies in relation to Information Governance remain up to date, reflect national guidance and are in operational use throughout Focus.
- Monitor organisational compliance with the UK GDPR/Data Protection Act
- Provide advice and assistance with regards to the completion of Privacy Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and organisational staff on matters relating to UK GDPR/Data Protection Act and the protection of personal information
- Assist in implementing essential elements of the UK GDPR/Data Protection Act such as the principles of data processing, data subjects' rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

2.4 All Supervising Staff

Supervisors will take responsibility for ensuring that the Information Governance Policy is implemented within their staff teams, ensuring that their staff, both permanent and temporary, are aware of:

- all information governance policies and guidance and their responsibility to comply with them;
- their personal responsibilities for information governance;
- where to access advice on matters relating to governance and confidentiality; and
- the security of their physical environments where information is processed or stored.

2.5 All Staff

It is the responsibility of each employee of Focus to adhere to the policy. Staff will receive instruction and direction regarding the policy from a number of sources including:

- Business Procedures
- Supervisor
- Specific training course
- Other communication methods, for example, team meetings
- Information on Workplace provided by the Information Governance Team
- New starter induction training from the Information Governance Team

Individual employees have a responsibility to ensure they are aware of all information governance policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any potential issues whereby a breach of security may occur.

3 INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK (IGMF)

3.1 Policies

Focus has developed a framework for its Information Governance Policy. This is supported by a set of information governance polices and related procedures to cover all aspects of information governance. The key information governance policies are:

Data Protection Policy: This policy sets out the roles and responsibilities for compliance with the UK GDPR/Data Protection Act 2018.

Confidentiality Policy: This policy sets out the principles that everyone who works at Focus and handles personal or confidential business information must follow. All staff must know how to keep information safe and respect the confidentiality of service users and carers, according to the law and the Social Care Record Guarantee. This policy also ensures that information held or processed by Focus is only shared with appropriate safeguards and in line with the terms and conditions agreed with the data providers.

Information Security Policy: This policy is to protect all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation.

Records Management and Data Quality Policy: This policy is to promote the effective management and use of information recognising its value and importance as a resource for the delivery of corporate and service objectives.

Social Media Policy: This policy acknowledges that many employees use social media for personal, professional and educational purposes. This policy aims to help all employees across the member organisations enjoy the benefits of social media, while being aware of their duties and responsibilities to their employer, colleagues, service users and carers.

3.2 Monitoring Compliance

Focus will monitor compliance with Information Governance requirements by:

- Reviewing the systems in place to develop and implement the Information Governance and related policies. Internal audit will support this process as appropriate.
- Including the reporting and investigation of reported Information Governance incidents
- Reviewing Information Governance requirements on a regular basis
- Undertaking an annual self-assessment using the NHS Data Security & Protection Toolkit (DSPT) and on-going monitoring of action plans.

3.3 Risk Management

All Information Governance incidents (e.g. disclosure of confidential information, theft of laptop, and unauthorised access to applications) must be reported through Focus' incident reporting procedure and in accordance with the IUC Alliance Risk Management Model Framework. The Head of Information Governance will co-ordinate any investigations. The investigation and results will be discussed by the leadership Group and/or where appropriate Professional Practice Governance Committee. Learning from risks and incidents is an important part of Focus' approach to quality assurance.

Information Asset Owners (IAO) and the DPO are expected to undertake risk assessments on data flows or information assets; ideally, but not exclusively within an Information Asset Register (IAR) to identify and report risks to the SIRO.

4 REVIEW AND MONITORING

This policy will be reviewed every 3 years or if there are changes to legislation.

5 IMPACT ANALYSIS

This policy will pay due regard to the following impacts:

5.1 Equality

In developing this policy, an equality impact assessment has been completed (See Focus IGMF). A full equalities impact assessment was deemed not to be required. This is because the policy is formatted in a way that is easy to read and can be made available on request in other formats and in other languages from the author of this framework. Arrangements can be made for members of staff with disabilities who wish to access information in a different format.
As a result of performing the analysis, the policy does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage.

5.2 Sustainability

The policy will pay due regard to any requirements during their activity and tendering of the Sustainability Impact Assessment, undertaking where appropriate.

5.3 Bribery Act 2010

Focus will be fully aware of the Bribery Act 2010, it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper. It is therefore, extremely important that staff adhere to this and other related policies and documentation outlined within their organisation, such as a Gifts and Hospitality Policy when considering whether to offer or accept gifts and hospitality and/or other incentives.

6 REFERENCE MATERIAL

- UK GDPR
- The Computer Misuse Act (1990)
- Human Rights Act 2018 (Specifically Article 8)
- Care Act 2014
- The Data Protection Act 2018
- The Copyright, Designs and Patents Act (1988)
- The Health and Safety at Work Act (1974)
- Investigatory Powers Act (2016)
- The Public Records Act (1958)
- NHS Code of Practice, The Common Law Duty of Confidentiality
- Mental Capacity Act (2005)
- NHS Information Governance: Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2020
- NHS England: The NHS Long Term Plan
- NHS Digital: A guide to confidentiality in health and social care: References - September 2020
- DHSC: Creating the right framework to realise the benefits for patients and the NHS where data underpins innovation - July 2021
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice