focus
independent adult social work

Data Protection Policy

Version 2.0

Heritage House, Fisherman's Wharf, Grimsby, DN31 1SY

CONTENTS

1. INTRODUCTION

1.1 Background

focus needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. This information includes name, address, email address, date of birth, private and confidential information, sensitive information. No matter how it is collected, recorded and used (on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018/General Data Protection Regulation (GDPR).

The lawful and proper treatment of personal information by focus is extremely important to the success of focus and in order to maintain the confidence of service users, carers and employees. focus will ensure it treats personal information lawfully and correctly.

1.2 Data Protection Principles

focus fully supports and complies with the eight principles of the Data Protection Act/GDPR which are summarised below.

Personal data**:-**

DPA 2018

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

GDPR

- Lawfulness, fairness and transparency - you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- Purpose limitation - you must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- Data minimisation - you must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- Accuracy - you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- Storage limitation - You must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why you collect this data.
- Integrity and confidentiality - You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.3 Scope

This Policy applies to all members of staff, Students/Placement/Agency staff, volunteers, contractors and sub-contractors and any other person representing or acting on behalf of focus.

2 . ROLES AND RESPONSIBILITIES

2.1 Senior Information Risk Officer (SIRO) / Head of Business and Governance

The Head of Business and Governance will be responsible for:

- Ensuring training is in place for those who handle personal information
- Ensure appropriate Data Protection procedures are in place
- Ensure risks associated with the protection of data through the Information Asset Register recommendations are reviewed.
- Ensure data flows are reviewed and approved by the board.

2.2 Data Protection Officer (DPO) / Head of Information & Security

The Head of Information & Security will be responsible for:

- Providing a clear line of reporting and supervision for compliance with data protection
- Ensure personal information is subject to data protection by design and by default through Data Protection Impact Assessments (DPIA), which are undertaken for projects collecting, storing, sharing or using personal information.
- Ensure any focus notifications to the Information Commissioner is updated to take account of any changes in processing of personal data
- Ensure data flow maps are undertaken of personal data and reviewed by the SIRO.

2.3 Employees

All employees will:

- Observe all guidance and procedures about the collection and use of personal information
- Collect and process appropriate information only in accordance with the purposes for which it is to be used by focus to meet its responsibilities
- Ensure the information is correctly input into focus computer systems
- Ensure the information is destroyed (in accordance with the provisions of the Data protection Act) when it is no longer required
- On receipt of a request from an individual for information held about them notify the Central Business Unit who will initiate the Subject Access to Records (SARs) procedure.
- Understand that breaches of this policy may result in Disciplinary action including dismissal.

3. POLICY REVIEW

This policy will be reviewed within a three year period as part of a rolling programme unless there are any changes in legislation.

4. INTERNAL REFERENCES

- Subject Access to Records Procedure

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 need to fully and be careful to ensure that under 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

External

- Current Data Protection Legislation
- General Data Protection Regulations (EU) 2016/679
- The Computer Misuse Act (1990)
- Human Rights Act 1998 (Specifically Article 8)
- Care Act 2014
- The Data Protection (Processing of Sensitive Personal Data) Order (2000)
- The Copyright, Designs and Patents Act (1988)
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- 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 2013
- NHS England: Everyone Counts: Planning for Patients 2014/15 to 2018/19
- NHS Digital: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- National Information Board and DH: Personalised Health and Care 2020
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice