focus
independent adult social work

Information Security Policy

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

CONTENTS

1 INTRODUCTION

1.1 Purpose

This document defines the Information Security Policy for focus. The policy applies to all business and covers the information, information systems, networks, physical environment and relevant people who support and use those business functions and in accordance with the Integrated Urgent Care (IUC) Alliance Information Governance Management Framework (IGMF). It provides the framework for information security risk management. The document:

- Sets out the focus policy for the protection of the confidentiality, integrity and availability of its assets, that is, hardware, software and information handled by information systems, networks and applications;
- Establishes the responsibilities for information security;

1.2 Scope

The scope of this policy is to ensure the security of focus' information assets. To do this focus will:

- Ensure availability – that assets are available for users;
- Preserve integrity - protect assets from unauthorised or accidental modification;
- Preserve confidentiality – protect assets against unauthorised disclosure.

This policy applies to all information media, systems, networks, portable electronic devices, applications, locations and users within focus. Wilful or negligent disregard of this policy may be investigated and dealt with under focus's Disciplinary Policy and Procedure.

2 DEFINITIONS

Confidentiality of Information: Person-identifiable, sensitive or otherwise valuable information will be protected against unauthorised access and disclosure

Information Assets: Any information that is stored physically or electronically, transmitted across networks or telephone lines, spoken in conversations or printed.

Integrity of Information: Safeguards to protect against unauthorised modification and destruction of information.

Physical, Logical, Environment and Communications Security: Controls to prevent unauthorised access, damage and interference to IM&T services and client records.

Infrastructure: Computers, systems, networks, cabling and other devices

3 DUTIES

3.1 focus Responsibilities

focus will ensure that appropriate arrangements are in place through its ICT provider, for the security of all key information, systems, networks and applications. It will also ensure implementation of this Security Policy and that the organisation and staff comply where relevant with:

- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- The Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Care Act 2014
- Crime and Disorder Act 1998

3.2 All Staff

All employees have a duty to:

- Safeguard hardware, software and information in their care
- Ensure that document files are not saved on the hard disk (including the desktop) of focus computers (if the computer were to be stolen the data would be lost).
- Ensure that person identifiable or other sensitive information is not stored on portable or removable media (laptops, USB, memory stick) under any circumstances.
- Prevent the introduction of malicious software on the organisation's IT systems;
- Report any suspected or actual breaches in security through the focus accident and incident reporting system;
- Comply with all focus information security measures. Deliberate misuse of information or systems, or negligently disregarding focus security measures could result in disciplinary action, including dismissal and may lead to a criminal conviction.

3.3 Supervisors

Supervisors are directly responsible for:

- Ensuring the security of focus' assets, (that is information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements;
- Ensuring that their staff are aware of their security responsibilities and comply with all focus policies and procedures;
- Ensuring that their staff has had suitable security training and training in the use of IT systems as appropriate

- Agree which staff are to be given authorisation to access specific IT systems and through the Central Business Unit, ensure passwords are issued and withdrawn as staff leave or change role
- Through the Central Business Unit that equipment is disposed of securely with all sensitive data removed

3.4 Caldicott Guardian / Chief Executive

The Caldicott Guardian's responsibility is to:

- Oversee the delivery of the focus Information Governance agenda to ensure that all information used within focus, but especially that relating directly or indirectly to service users / carers is managed carefully, responsibly, within current law and with due regard to considerations of privacy such as those defined in the Caldicott principles.
- Ensure that all staff are consistently made aware of their obligations in this area
- Ensure security is considered when applications and systems are under development or enhancement.

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

The Head of Business and Governance will ensure that:

- This policy is implemented across focus, monitoring and reporting on the state of information security and that procedures are developed to maintain security
- All risks associated with information is identified, reviewed and appropriately responded to;
- Critical information assets (SystmOne, ContrOCC) have appropriate business continuity plans and disaster recovery plans
- Ensure an asset register is maintained of physical equipment and software

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

The Head of Information & Security will:

- Inform and advise leaders and employees about obligations to comply with the GDPR and other data protection laws;
- Ensure the monitoring of compliance with the GDPR and other data protection laws, and data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- Provide advice on, and monitor data protection impact assessments;
- Cooperate with the supervisory authority; and
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

3.7 ICT Service Suppliers

Focus will ensure that ICT suppliers will on its behalf ensure that:

- Information systems, applications and networks are available when needed and can be accessed only by legitimate users;
- Protecting hardware, software and information assets under its control;
- All necessary steps are taken to ensure that the information systems, applications and networks are able to withstand or recover from threats to their availability, integrity and confidentiality.
- The information systems do not pose an unacceptable security risk to focus;
- Measures are in place to detect and protect the network from viruses and other malicious software;
- Connections to external networks and systems are documented and approved
- Implement and maintain device control on every focus computer
- All operational applications, systems and networks are monitored for potential security breaches
- That information systems are regularly checked for compliance with security implementation standards
- Disaster recovery plans are in place for all critical applications, systems and networks
- Ensure all portable storage devices and removable media supported by focus are encrypted at hard disc level

4 PRINCIPLES

4.1 Risk Assessment and Audit

Risk assessments will be carried out by the ICT service supplier in relation to the business processes covered by this policy. These will cover all information systems, applications and networks that are used to support these business processes.

The NHS Data Security & Protection Toolkit (DSPT) requires focus to undertake a self-assessment audit based on defined indicators.

All information security incidents will be reported and investigated under the focus accident / incident reporting system and through the ICT supplier reporting and investigation mechanisms where appropriate.

4.2 Operating Procedure

Procedures relating to the operation of systems must be documented. User access control and access rights will be developed for each individual system. No external agency will be given access without explicit permission

4.3 Unauthorised Software

Use of any non-standard software on focus equipment must be approved in advance by the Head of Information & Security. All software used on focus equipment must have a valid licence agreement.

It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action.

4.4 Mobile Computing and Communications

Equipment in transit is at particular risk of being damaged, stolen or lost. Supervisors will advise staff as to how to mitigate these risks. Mobile devices should not be used under any circumstances to store client, person or sensitive electronic data.
All users are to hold all data on the central server and not store data to local drives.

4.5 Electronic Transfer of Person Identifiable Data

Any bulk electronic extract and transfer of person identifiable or sensitive data by portable or removable media, file transfer protocol or email, must be authorised in advance by the Head of Information & Security. Any such transfer must be encrypted.

4.6 Removable Media

(e.g. USB, memory stick, pen drives, external hard disk drives, CD Rom, floppy disk, mobile phones, smart phones, audio devices etc)
Staff and contractors are not permitted to introduce or use removable media for storing or transfer of person identifiable or sensitive information. Supervisors are responsible for the day to day management and oversight of removable media used within work areas to ensure this policy is followed. They are responsible for the secure storage of all portable electronic media and safe disposal through the ICT service provider.

No discs should be uploaded unless they have been virus checked.

4.7 Email and Internet

The use of web based email such as 'hot mail' and 'mail.com' is prohibited for the use of any official information belonging or relating to focus. Use of the internet will be monitored and technical controls will be put in place to ensure focus information resources are protected from malicious attack.

4.8 Reporting Data Security Breaches and Weaknesses

Data security breaches and weaknesses, such as the loss of data or the theft of a laptop, must be reported in accordance with the focus accident and incident reporting system and, where necessary, investigated by the Head of Business and Governance or the ICT provider where appropriate.

4.9 Training

All staff will be provided with security awareness training on a 3 yearly basis, through an on line package, that will include Caldicott, Data Protection and reporting of security incidents. Training on information security is part of the induction programme for new staff.

5 REVIEW AND MONITORING

This policy will be reviewed if there are changes to legislation and/or difficulties in practical application.

6 IMPACT ANALYSIS

This policy will pay due regard to the following impacts:

6.1 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.

6.2 Sustainability

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

6.3 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.

7 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