Information Technology Policy

Issued by:	Approved by:
IT Department	Executive Board of Directors
Date: July 2018	Date: 29th August 2018
Policy Version:	**Date for Review:**
6.0	July 2021

Contents

Introduction 2
Data Protection When Using IT Systems 2
Equipment & Software 2
Local Equipment Security 3
Virus Protection 3
Use of External NHS Systems 3
Third Party Access 4
Use of Pilgrims Hospices Remote Working Devices 4
Passwords and Access Security 4
Security Incidents 5
Failure to Comply 5
Related Policies 5

WHO DOES THIS POLICY APPLY TO?

This policy applies to all staff, volunteers, Trustees, agency workers, self-employed workers and third parties of Pilgrims Hospices; hereafter referred to as “Users”.

HOW WILL THIS POLICY BE COMMUNICATED?

This policy will be communicated via Select HR and will be uploaded to the Pilgrims Hospices Intranet.

Introduction

Pilgrims Hospices uses Information Technology (IT) across the organisations’ functions as an aid to meeting its business objectives.

This policy outlines the expectation of all Users when using IT for Pilgrims Hospices business purposes, the data protection surrounding the information held on electronic equipment and software, and the processes Users should take when using IT in their daily activities.

Users should ensure they read and understand this policy, and familiarise themselves with additional relevant IT policies referenced in this policy.

Data Protection When Using IT Systems

Pilgrims Hospices takes the processing, storing and handling of data extremely seriously, and understands that IT systems can play a crucial role in ensuring the confidentiality, security and integrity of information.

It is expected that all staff are aware of and comply with current data protection regulations and guidelines that include but are not limited to:

- The Data Protection Act
- The General Data Protection Regulations (GDPR).

Access to any confidential information should be handled in accordance with Pilgrims Hospices existing confidentiality policies. Access should only be given to those who need it to successfully perform the requirements of their role.

Users should ensure that all data is stored and processed on the official Pilgrims Hospices network drives to ensure that it is secure and easily recoverable for business continuity reasons.

Equipment & Software

All requests for IT related equipment and software must be made in writing to the IT Department in a timely manner to ensure there is sufficient funding and availability.

All computer systems should be used in compliance with the guidance outlined in this document.

Any information or IT equipment provided by Pilgrims Hospices that is not used to conduct official Pilgrims Hospices business may be subject to removal at any time.

The IT Department maintains a register of IT assets and where these are installed, which includes a register of the current Users who have had IT equipment assigned to them. This is in order to track and manage Hospice technology assets. No item of computer equipment may be reassigned, moved, borrowed, disposed of or changed without the knowledge and express approval of the IT Department.

All information will be removed from IT equipment scheduled for disposal and any devices holding information will be destroyed. Any data or software will be removed from re-allocated equipment where such data or software is no longer needed.

All Pilgrims Hospices computer equipment is set up by the IT Department. The configuration settings set by the IT Department must not be amended.

Upon a User's contract being terminated with Pilgrims Hospices, or when equipment is no longer required to fulfil a User's current role any equipment must be returned to the IT department or the User's Line Manager before the end of their contract.

As its IT facilities are used to benefit the conduct of its business, Pilgrims Hospices reserves the right to monitor the operation of all its systems, (including all e-mails sent and received and Internet access), to access all records within them, and to retain or dispose of those records as it deems necessary. Users must not, therefore, expect personal privacy in anything they create, send, receive or download onto a Pilgrims Hospices' computer or network.

Local Equipment Security

Each User is responsible for taking reasonable precautions to secure any computer equipment assigned to them from theft or abuse.

If due to unforeseen circumstances Users experience any loss or damage to Pilgrims Hospices IT equipment they must report it to their Line Manager and to the IT Department as soon as possible. This will ensure that any data held on the equipment can be securely wiped.

Virus Protection

Virus protection software is installed on all Pilgrims Hospices PC's and servers. This is automatically kept as up to date as possible, but this is not a guarantee against a virus entering the network.

If a User considers that a virus has entered the network, they must inform the IT Department immediately.

Use of External NHS Systems

Selected employees will have access to some NHS and other external health systems. The terms of this policy apply to the use of those systems as well as any other conditions set out by the service provider. These systems should be the only methods of processing patient data outside of existing Pilgrims Hospices internal systems.

Those who need it will be given access to the NHS secure e-mail system, NHS Mail.

The use of these systems is to assist solely in the care of Pilgrims Hospices' patients and Users' must on no account look up information for any other purposes.

Third Party Access

Access to Pilgrims Hospices information systems by third parties shall be strictly controlled.

Under no circumstances must third parties be allowed unauthorised access and, except in emergencies, must have signed a mutually agreed confidentiality agreement before commencing work.

All third parties who may require remote access to support and maintain communications systems shall be required to commit to using qualified representatives and to maintaining confidentiality of data and information at all times.

The method of access shall be through a secure connection only. Any access of this type must be approved by the IT Department, who must be informed every time the link is required.

Use of Pilgrims Hospices Remote Working Devices

For Users who use Pilgrims Hospices IT systems and equipment remotely, or offsite they should ensure they read and understand the terms outlined in the Pilgrims Hospices Offsite Working and Removable Media Policy.

Passwords and Access Security

Passwords are used throughout the organisation to access Pilgrims Hospices computer systems.

Passwords must be at least 8 characters long, cannot be the same as a previous password and must contain characters from at least three of the following:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters on the keyboard (ie. £$%^&*)

To ensure security, commonly used words and names should not be used for passwords, and instead long and complex passwords should be used so that they cannot be easily guessed by others. Passwords should not be shared at all with others.

Passwords will be prompted to be changed every 60 days.

Security Incidents

If a User encounters a security incident with a Pilgrims Hospices IT system or piece of equipment, they must ensure that they inform their Line Manager and the IT Department as soon as possible.

Where an IT Security incident occurs which may lead to a personal data breach, Users should ensure they follow the procedures outlined in the Pilgrims Hospices Data Breach Policy.

Failure to Comply

Any User who is seen to be in breach of the terms and conditions outlined in this policy may be subject to disciplinary action, in accordance with the Pilgrims Hospices Disciplinary Policy and Procedure.

Related Policies

- Offsite Working and Removable Media Policy
- Acceptable IT Use Policy
- Disciplinary Policy and Procedure
- Data Breach Policy
- Confidentiality Policy
- Data Protection Policy
- Leavers Policy and Process

All staff retain the right to discuss the contents of this policy with Management at any time.