Woking & Sam Beare
Hospice and Wellbeing Care

INFORMATION SECURITY POLICY

Policy / procedure code:	ICT001
Version:	3
Policy owner:	IT Manager
Approval Date:	April 2021
Ratified by:	Governance Committee
Next Review Date:	April 2024
For Information and action to:	All staff, volunteers and 3rd party representatives

Version Control Sheet

Policy / Procedure: Information Security Policy

Version	Date	Author	Status	Comment
V1	01/11/2015	Paul Bartlett	Approved	
V2	20/12/2017	Paul Bartlett	Approved	
V3	19/04/2021	John Sullivan / Julie Gardner	Approved	Full review and updated legislation.

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version on the R Drive is the controlled copy. Any printed copies of this document are not controlled. As a controlled document this document should not be saved onto another drive and should only be accessed from the R Drive: ..\..\POLICIES & GUIDELINES\IT\ICT001 ICT Security Policy.pdf

Contents **Page**

1. Introduction

Woking and Sam Beare Hospices (WSBH) is a charity providing palliative and end of life care. Information processing is a key element to enable delivery of services and other business activities to support funding. It is therefore important that the organisation has a clear and relevant Information Security Policy. This is essential for compliance with data protection and other legislation and to ensure that confidentiality is respected.

The purpose of the Information Security Policy is to protect all information assets to a consistently high standard.

This Policy should be read in conjunction with the Information Governance Framework (IG01) and:

- ICT002 Mobile and Remote Access Policy
- IG02 Data Protection and Confidentiality Policy
- IG04 Clinical Records Management
- IG08 Notification of Data Security and Protection Incidents Policy

1.1 Scope

This policy covers:

- All Information and Communications Technology (ICT) equipment at any site managed by WSB Hospices
- All equipment owned by WSBH
- All equipment owned by individuals that is used to access WSBH ICT networks or equipment
- All employees, volunteers, contractors and information service providers and anyone accessing WSBH network or using any equipment managed or owned by WSBH

This policy applies to all types of information assets including but not limited to:

- Digital or hard copy patient health records (including those concerning all specialties and GP medical records)
- Digital or hard copy administrative information (including personnel, estates, corporate planning, supplies ordering, financial and accounting records)
- Digital or printed X-rays, photographs, images and imaging reports
- Digital media (including data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, and other internal and external media compatible with NHS information systems)
- Computerised records, including those that are processed in networked, mobile or standalone systems
- Email, text and other message types

2. Aim and Objectives

2.1. Aim

The aim of WSBH Information Security Policy is to preserve:

- **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.

2.2. Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WSBH by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other associated policies
- Describing the principles of security and explaining how they shall be implemented in the organisation
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business
- Protecting information assets under the control of the organisation

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Senior Information Risk Owner (SIRO) of WSBH but, on a day-to-day basis, the IT Manager shall be responsible for managing and implementing the policy and related procedures.

3.2. Information Asset Owners (IAO) are responsible for ensuring that permanent and temporary staff, volunteers and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the IT Manager and approved by the Governance Committee.

3.5. Line Managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.6. Each member of staff shall be responsible for the operational security of the information systems that they use.

3.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information that they use is maintained to the highest standard.

3.8. Contracts with external contractors shall be in place before access is allowed to the organisation's information systems. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4. Legislation

4.1. WSBH is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of WSBH who may be held personally accountable for any breaches of information security for which they may be held responsible. The WSBH shall comply with the following legislation:

- General Data Protection Regulation (UK)
- The Data Protection Act (2018)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2012

5. Policy Framework

5.1. Management of Security

- The Chief Executive is ultimately responsible for Information security. This responsibility is discharged through the designated roles of SIRO and IT Manager as required by the Information Governance Data Security and Protection Toolkit.
- The SIRO is responsible for Information Security and advises the Board on the effectiveness of information risk management across the organisation.
- The IT Manager shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- Data Security and Protection Training is mandatory and all staff are required to complete online Data Security Awareness training every 2 years
- All staff are required to read the Information Governance Policy when completing the relevant mandatory training module and accept the declaration.

5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job descriptions.

5.4. Security Control of Assets

Each IT asset (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

5.5. Access Controls

Authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.6. User Access Controls

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

5.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.8. Application Access Control

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 licence from the supplier.

5.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be identified, registered and physically protected from threats and environmental hazards.

5.10. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Management Team.

5.11. Information Risk Assessment

All Information assets will be identified and assigned an IAO. IAOs shall insure that information risk assessments are performed at least annually, following guidance from the SIRO. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review.

5.12. Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be recorded on WSBH Incident Reporting Tool and reported to the Management Team. All information security events, near misses and suspected weaknesses are to be reported and investigated to

establish their cause and impacts with a view to avoiding similar events. Incidents will be reported the Information Commissioners Office (ICO) where required as per the Hospice Notification of Data Security and Protection Incidents Policy IG08.

5.13. Classification of Sensitive Information.

WSBH will implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Data Security and Protection Toolkit (DSPT) to secure its information assets.

	CONFIDENTIAL	RESTRICTED
Identification	• Documents should be watermarked 'Confidential'. If in a sealed envelope this should also show 'Confidential' in top left corner.	• Documents should be watermarked 'Restricted'. If in a sealed envelope this should also show 'Restricted' in top left corner.
Type of information	• Identifiable individual's financial information • Clinical patient records • Identifiable patient clinical information • All personal and sensitive data	Any information that: • Adversely affects the reputation of the organisation or its officers or may cause substantial distress to individuals • Makes it more difficult to maintain the operational effectiveness of the organisation • Causes financial loss or loss of earning potential, or facilitates improper gain or disadvantage for individuals or organisations • Prejudices the investigation, or facilitate the commission of crime or other illegal activity • Breaches proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies • Breaches statutory restrictions on disclosure of information • Disadvantages the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

	CONFIDENTIAL	RESTRICTED
Storage: physical	• Information must be stored in a locked room or cupboard to which only authorised persons have access.	• Information must be stored in a locked cabinet or cupboard.
Storage: electronic	• Information must be saved in a folder controlled by access rights. • Individual files outside of a secure folder must be password protected. Memory sticks, if used, must be password protected and encrypted.	• Information must be saved In a folder controlled by access rights.
Printing	• Printing is via a print queue and must only be released to the user that has sent the print job. Sharing of ID cards that release print jobs is forbidden.	
In transit: physical	• Information must be transported securely in sealed packaging or locked containers. • If using an internal mail folder, documents should additionally be in a sealed envelope. • Documents not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.	
In transit: electronic	• Special permission must be obtained from either the Caldicott Guardian or SIRO for sending confidential information outside of the EU. • Emails to/from NHS organisations must be sent securely and encrypted. • File transfer systems must not be used.	• If information is sent by email the addressee must be an individual and not a generic email address (such as info@...).

5.14. Protection from Malicious Software

WSBH shall use software countermeasures and management procedures 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 in writing (including emails) from the IT Manager.

5.15. User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the IT Manager before they may be used on WSBH systems. Such media must also be fully virus checked before being used on the organisation's equipment.

5.16. Monitoring System Access and Utilisation

An audit trail of system access and data used by staff shall be maintained and reviewed on a regular basis.

WSBH will regularly monitor and audit compliance with system access usage. WSBH reserves the right to monitor activity where it suspects that there has been a breach of policy.

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employee electronic communications (including telephone communications) for the following reasons:

- Establishing factual information
- Investigating or detecting unauthorised use of the system(s)
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above Act and the Human Rights Act.

5.17. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks are approved by the IT Manager before they commence operation.

5.18. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Management Team.

5.19. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the IT Manager. Users shall not install software on the organisation's property without permission from the IT Manager.

5.20. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.21. Reporting

The IT Manager shall keep the Management Team informed of the information security status of the organisation by means of regular reports and presentations.

6. Monitoring

Compliance with this policy will be monitored via the Governance Committee. This policy shall be subject to audit by the Management Team.

7. Equality Impact Assessment

WSBH is committed to creating a positive culture for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment, pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

PROTECTED CHARACTERISTIC	EQUALITY IMPACT ASSESSMENT
Age	There is no evidence to indicate that any staff member or volunteer represented in these Protected Characteristic groups is, as a result of this Policy, affected more or less favourably than staff and volunteers in other groups
Gender	
Gender Re-assignment	
Sexual Orientation	
Race	
Religion or Belief	
Marriage / Civil Partnership	
Pregnancy / Maternity	
Disability	