WOKING & SAM BEARE HOSPICES

ICT001: ICT SECURITY POLICY

Policy / procedure code:	ICT 001
Version:	V1
Ratified by:	20/12/17
Name of policy owner:	Paul Bartlett
For Information and action to:	All staff, volunteers and 3rd party representatives
Name of originator / author:	Paul Bartlett
Issue date:	01/11/15
Last review date:	
Review by date:	01/11/2016

WOKING & SAM BEARE HOSPICES

Version Control Sheet

Policy / Procedure: ICT001: ICT Security Policy

Version	Date	Author	Status	Comment

Signature Sheet

Policy / Procedure Name: ICT Security Policy

Code: ICT001 **Version: 1**

Date	Name	Designation / Post	Department	Signature

Acronyms:	
WSB - Woking and Sam Beare	SIRO – Senior Information Risk Owner
DPA - Data Protection Act	IAO – Information Asset Owner

1. Introduction

This top-level information security policy is a key component of WSB Hospices' overall Information Governance framework and should be considered alongside other relevant documents especially ICT002 Mobile and Remote Access Policy, and the IG 04 Information Governance Framework

Records Management

WSB Hospices is a multi-site organisation that also provides healthcare services to patients in their own home or at locations not managed by WSB Hospices. This policy covers:

- All ICT equipment at any site managed by WSB Hospices.
- All equipment owned by WSB Hospices.
- All equipment owned by individuals that is used to access WSB Hospices ICT networks or equipment.
- All employees, volunteers, contractors and information service providers and any one accessing WSB Hospices network or using any equipment managed or owned by WSB Hospices.

Additionally, 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, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);
- Digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
- Digital media (including, for example, 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. Objectives, Aim and Scope

2.1. Objectives

The objectives of WSB Hospices Information Security Policy are 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. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WSB Hospices by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other 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 **S**enior **I**nformation **R**isk **O**wner of WSB Hospices, but on a day-to-day basis the IT Manager shall be responsible for managing and implementing the policy and related procedures.

3.2. **I**nformation **A**sset **O**wners are responsible for ensuring that their 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 ICT Security Policy shall be maintained, reviewed and updated by the IT Manager and approved by the Corporate Governance Group. This review shall take place annually.

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 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 they use is maintained to the highest standard.

3.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. 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. WSB Hospices 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 WSB Hospices, who may be held personally accountable for any breaches of information security for which they may be held responsible. The WSB Hospices shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- 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 2001

5. Policy Framework

5.1. Management of Security

- At board level, responsibility for Information Security shall reside with the SIRO.
- 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.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

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 definitions.

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

Only 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 bona-fide business need to access the information. Access controls will be granular and based on Active Directory security groups and folder level permissions.

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 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 Information Governance Management Group

5.11. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of WSB Hospice's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. Information security events and weaknesses

All information security events and suspected weaknesses are to be recorded on WSB's Incident Reporting Tool and reported to the IGOV Management Group. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.13. Classification of Sensitive Information.

WSB Hospices will implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their 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 esp. bank details • patients' clinical records	Any information that: • adversely affects the reputation of the organisation or its officers or

	• patient identifiable clinical information • all personal and sensitive data	cause substantial distress to individuals; • make it more difficult to maintain the operational effectiveness of the organisation; • cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations; • prejudice the investigation, or facilitate the commission of crime or other illegal activity; • breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies; • breach 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.
Storage - physical	In a locked room or cupboard to which only authorised persons have access.	In a locked cabinet or cupboard.
Storage – electronic	In a folder controlled by access right. Individual files outside of a secure folder must be password protected. Memory sticks, if used, should be password protected and encrypted.	In a folder controlled by access rights.
Printing	All printing of sensitive classified documents must be printed to a password protected print box or to a user's local printer. All measure to eliminate the likelihood of material being left uncollected on a printer must be carried out.	
In transit – physical	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 IT manager for sending Confidential information outside of the EU.	If sent by email the addressee must be an individual and not a generic email address (such as info@...).

	If sent by email the addressee must be an individual and not a generic email address (such as info@...). Emails to/from NHS organisations must be sent securely and encrypted. File transfer systems should not be used.	

5.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat 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. Users breaching this requirement may be subject to disciplinary action.

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 WSB Hospices systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

5.16. Monitoring System Access and Use

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

WSB Hospices has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right 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 employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- 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 Information Governance Management Group

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. Users breaching this requirement may be subject to disciplinary action.

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 Information Governance Management Group informed of the information security status of the organisation by means of regular reports and presentations.

5.22. Policy Audit

This policy shall be subject to audit by the Information Governance Management Group.

5.23. Further Information

Further information and advice on this policy can be obtained from the IT Manager