Southern Hampshire
PRIMARY CARE ALLIANCE

IT Equipment Loan Policy

1.2

Document Type:	Policy & Procedure
Current Status:	Final
Version:	1.2
Reviewed by:	Lee Busher
Latest review date:	July 2022
Original author:	Lisa Baker
This version approved:	July 2022
Next review due:	July 2024
Approved by	Kerry Cooper/Kathryn Bannell
Original publication date	September 2021
Applies to:	All Southern Hampshire Primary Care Alliance Staff

Version Control

Version	Date	Author	Change Summary
0.1	01/08/2021	Lisa Baker	First Draft
1.0	30/08/2021	Lisa Baker	Second Draft – SW Amendments
1.1	29/09/2021	Lisa Baker	Final with sign off
1.2	21/07/2022	L Busher	Formatting changes and review

Contents

1. PURPOSE

The purpose of this document and its associated policy "Southern Hampshire Primary Care Alliance (SHPCA) Computer, Email & Internet Usage Policy" are to inform those personnel in scope of their responsibilities for contributing to the security of the information we work with and the standards of acceptable use of loan equipment for computing and the use of communications devices or systems.

2. SCOPE

This document applies to workers and contractors engaged to provide a service to the organisation and contracted directly by SHPCA. the Loaning of equipment,

3. DEFINITION

SHPCA Corporate Equipment Loan Policy, together with this standard is the minimum standard for acceptable use which should be appliedwhenever those individuals in scope access SHPCA or its partners' information, facilities, and equipment.

In addition, local procedures, standards, and work instructions may be defined to allow flexibility of organisational practices. This policy provides a minimum requirement to be met under nationally recognised standards.

4. TERMS

- ✓ **Information Security** is about avoiding harm to people, customers, or our businessby protecting the information we use. This is achieved by considering:
- ✓ **Confidentiality** - Information held by SHPCA must only be seen by those who are authorised and have a business need to access as part of their role.
- ✓ **Integrity** - Information used and provided by SHPCA can only be modified by those authorised to do so and it is accurate, up- to-date and relevant.
- ✓ **Availability –** Information required is accessible when needed.
- ✓ **Computing and communications devices or systems** for the purposes of this standard encompasses all those devices and applications normally used to access,store, create or transmit information. Examples are desktop computer, laptop, tablet, mobile phone, smartphone, telephone, digital camera, digital video recorder,internet access, e-mail, social networking sites, applications, mobile apps and removable storage and network storage.
- ✓ **The EU General Data Protection Regulation (GDPR**) requires any organisation that processes data on identifiable living people to comply and be able to demonstrate compliance with the six enforceable principles. GDPR gives control to citizens and residents over their personal data and simplifies the regulatory environment for international business by unifying the regulation within the EU. It is important to protect physical and electronic records which either contain Personally Identifiable Information (PII) or information which can likely lead to the identification of an individual. GDPR covers several areas such as citizen records, websites, internet activity, recruitment and selection of staff, employment records, information about employees' health and CCTV systems or information which together with other

information in the possession of the received of that information could lead to the identification of an individual.

- ✓ The **Data Controller** (also known as **Information Asset Owner** or **Owner)** is a DPA term and is the role or group accountable for the management of the information. This is not to be confused with the **Subject** which is the person or object being described by the information.
- ✓ **Information Classification** is the act of deciding the sensitivity of the informationasset. This is usually done by the information owner considering the harm/consequence if the information asset were lost, stolen, or disclosed without authorisation.
- ✓ Appropriate **Information Handling** is the set of actions which are associated witha classification.

5. RESPONSIBILITIES AND ACCEPTABLE USE

5.1 General Principles

The following standard sets out arrangements about SHPCA expectation concerning the security of the information and equipment we use, the environment in which we work and the use of computing and communications devices or systems. You must treat paper-based and electronic information with equalcare.

SHPCA policies are published on intranet and you should speak to a manager for further advice.

5.2 Portable IT Assets

Laptops, mobile phones and smartphones and other portable devices must not beleft unattended. They must not be left in sight in cars, public transport, or hotels. They should not be kept on desks overnight; they must be stored in locked cupboards/drawers or taken home. They must not be left in vehicles overnight.

Loss of equipment must be reported as soon as possible to the IT Team on 023 92 414 020

5.3 Computer Use

No exhaustive list can be prepared defining all possible forms of misuse of computing and communications devices or systems. The individual circumstances of each casewill need to be considered. However, some examples are outlined below:

- ✓ Use of computing resources for improper, immoral, fraudulent, or unlawful purposesor to access, store, create or transmit any material which is offensive, abusive, indecent, defamatory, obscene, or menacing. For example, sexually explicit material or offensive statements based upon race, sex, sexuality, disability, age, orreligion.
- ✓ Storing/loading/executing of software for a purpose which is not work related.
- ✓ Storing/loading/executing of software:
- ✓ which has not been acquired through approved SHPCA procurement procedures, or
- ✓ for which SHPCA does not hold a valid programlicence, or
- ✓ which has not been the subject of formal virus checking procedures.

- ✓ Storing/processing/printing of information for a purpose which is not work related.

5.3.1 Obtaining Computer Equipment and Software

SHPCA can provide a loan laptop for the purpose of remote working. Line managers will need to email the IT Manager. If there is equipment available to loan the IT team will complete a Laptop/Equipment Check Out form and present with the equipment to the staff member. They must then check everything on the form is correct and agree to the T&C's by signing and dating the form. This is then kept on file until the return of the equipment see appendix1

Loss of equipment or faults with any supplied hardware or software must be raised with the IT Team as soon as possible.

5.3.2 Credentials and Systems Access

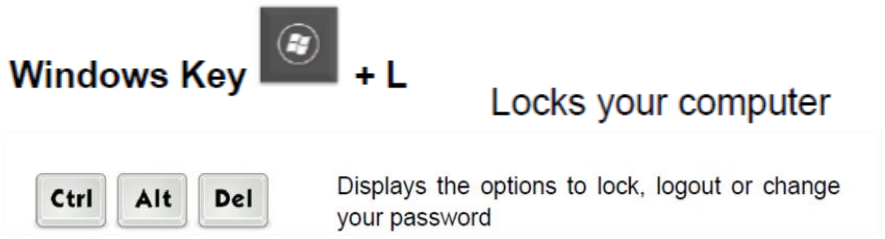
When issued with loan equipment will receive a user guide, login details and a temporary password. This password MUST be changed at first log on.

It is a criminal offence under the Computer Misuse Act, 1990 to deliberately attempt to access a system to which you have no authority.

5.3.3 Unattended Equipment

Computer equipment that is logged on and left unattended can present a tempting target and gives people access to systems you use. Unauthorised access of an unattended laptop/pc can result in harmful or fraudulent use.

Equipment should therefore always be safeguarded appropriately – especially when left unattended.

- ✓ Remove your smartcard.
- ✓ lock or log out of your computer prior to leaving it unattended.
- ✓ Do not wait for the screensaver.
- ✓ 

- ✓ Screen locks/savers must be password protected and may only be suspended whilst delivering presentations.
- ✓ Log out of all cloud based accounts – NHSMail, Teams, Office to avoid you information getting into the wrong hands.

5.3.4 Clear Desk Policy

SHPCA must adhere to the Clear desk policy. The Clear Desk Policy is to prevent unauthorised access to sensitive personal and/or confidential information.

5.3.5 Working Remotely

SHPCA employees must observe the points below when working away from the office.

This applies to your use of any SHPCA communications facilities whenever you are working remotely.

When you are working remotely, you must:

- ✓ Obtain authorisation before taking personal or sensitive information away from our offices.
- ✓ Not leave equipment and files unattended in public areas.
- ✓ Not use their own personal computer to work on personal identifiable data or sensitive corporate information.
- ✓ Position yourself so that your work cannot be overlooked by any other person.
- ✓ Ensure that sensitive information is not overheard, especially in public areas.
- ✓ Not load unauthorised software onto the laptop or device without permission.
- ✓ Not discuss or show sensitive SHPCA information tothose with no right to know.
- ✓ Take reasonable precautions to safeguard the security of your laptop computers and any computer equipment on which you do SHPCA business, locking equipment and sensitive information away or storing out of sight
- ✓ Not download or save any data to home storage devices or upload to cloud storage or backup services (such as, but not limited to, personal O365 accounts, Dropbox, Box, Google drive, Huddle, etc.).
- ✓ Inform their Line Manager as soon as possible if records, equipment, or any computer equipment on which you process SHPCA work has been stolen.
- ✓ Ensure that any work which you do remotely is saved on SHPCA system or is transferred to SHPCA systems, as soon as is reasonably practicable.
- ✓ Ensure that ID badges, remote access tokens or memory sticks are kept separatelyfrom computer equipment when not in use.
- ✓ Ensure the issued equipment is not used by others i.e., family and friends, etc

It is your responsibility to check that the performance and reliability of your internet connection is adequate for working remotely and contact your internet service providerto resolve issues.

Homeworkers who are using Company supplied and supported equipment can receive telephone support from Healthcare Computing on 03450348690 they are available 7 days a week 08:00am - 08:00pm, if the issue cannot be resolved by telephone, they will be required to bring the equipment to our offices, as home visits are not possible. It is not possible for SHPCA to provide support for equipment owned by members of staff.

- ✓ Removable media is a common route for transferring malicious software such as viruses, you must not use personal removable media devices to transfer files between your personal computer and SHPCA computers
- ✓ Removable Media must be scanned for malicious software before opening or transferring files: Right Click and Select “Scan for Threats….”
- ✓ Only memory USB sticks issued to you by SHPCA are authorised to be used.

6. COMPLIANCE

Failure to follow the procedures described in this document may impact on good employee relations and the reputation of Southern Hampshire Primary Care Alliance. Appropriate action (including disciplinary) will be taken if there is a breach in policy.

7. REVIEW AND REVISION

This standard will be reviewed as it is deemed appropriate, but no less frequentlythan every 36 months.

Policy and procedure review will be undertaken by the SHPCA Corporate IT Group and Information Governance Group.

8. USEFUL CONTACTS

On Call

Healthcare Computing	IT Support	03450348690
Lisa Baker	IT Manager	07880366614
Office		02392 414020

9. APPENDIX 1

LAPTOP/EQUIPMENT CHECKOUT FORM

1. This form is required for staff who wish to loan SHPCA equipment t enable remote working

2 Any staff member that is issued a laptop or any other equipment will be responsible for its care and security

3. Please list the items that are being checked out

Equipment	Serial Number	Reason for Loan

4. Date of Loan: Date to be returned (if applicable):

I understand that the following conditions will apply

a. I will return the equipment to the hub no later than the date indicated above.

b. I will exercise reasonable care when transporting and using the equipment.

c. I understand that if I no longer work for SHPCA I will return the equipment.

d. I understand that there is to be no patient information saved/stored on the laptop

e. I understand that the equipment is ONLY for the purpose of my role.

Staff member/Clinician (Please Print) Date:

Signature: Phone Number:

SHPCA Approval		
Equipment Issued by:		Date:
The item(s) have been returned and inspected		
All Accessories have been returned?	Y/N	If no why?
Received By:		Date:

This form will remain on file while the equipment is on loan