St Andrew's Healthcare

Acceptable Use Standard

Title of Document: ACCEPTABLE USE STANDARD V1.6
Owner: SIRO
Author: CISO
Brief Description of Document: Policy which mandates the approach and frameworks towards the acceptable use of Charity Assets
Classification: INTERNAL
Date of Release: 03/12/2022
Next review date: 03/03/2025
Retention of Archive Copies: 1 Year (Unless retained for contractual requirements)

Contents

Purpose

This standard determines the acceptable use of Assets within St Andrew's Healthcare (StAH).

Scope

Individuals or groups (known as 'Users' for the purposes of this document) covered by this standard include, but are not limited to:

- All StAH employees working for, or on behalf of StAH
- All 3rd Party organisations and contractors working for, or on behalf of StAH

Information and information processing assets (known as 'Assets' for the purpose of this document) covered by this standard include, but are not limited to:

- All devices used for the provision or access of StAH services, including any 3rd party services.
- The use of all StAH devices, including any 3rd party devices.
- The use of personal devices on StAH premises.
- The use of StAH user accounts.
- The use of StAH company data or information (with the exception of public data).

Management Statement

The appropriate use of StAH's assets ensures that StAH can meet its operational obligations, and customer requirements. In addition, appropriate use of these assets decreases the risk of financial, reputational or organisational consequences caused by misuse. Therefore, it is essential for those who are custodians of assets to be aware of their responsibilities to maintain the confidentiality, integrity, availability and lawful handling or use of that asset.

As a rule of thumb (and in the absence of any specific policy or instruction), when using IT systems and handling information, your actions/activities must not raise the risk of any harm towards the integrity of StAH's interests, data, assets, reputation or financial status.

To suitably mitigate these risks, StAH must have in place effective acceptable use controls with the ability to detect and handle asset misuse.

Any unauthorised deviation from this standard and supporting documentation may result in disciplinary action for staff, and sanction for contractors and 3rd party suppliers.

Policy Requirements

To ensure compliance with the Information Security Policy, StAH must implement and ensure:

- StAH's approach towards Acceptable Use satisfies the appropriate controls and activities defined within StAH's ISO27001 Information Security Management System and mitigates those risks which impact the Confidentiality, Integrity and Availability of StAH's information processing assets.
- All acceptable use activities within StAH are aligned to recognised methodologies underpinned by a robust and succinct suite of supporting standards, processes and procedures.
- All assets used within StAH have clearly articulated, communicated and robust terms of use (i.e. responsibilities, handling).
- Technical and administrative controls must be in place to detect and formally handle suspected or confirmed cases of asset misuse.

Annex A – Acceptable Use Requirements

Principles of Use, Ownership and Custody of StAH's Assets

The following activities are, in general either mandated or prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities, whereby these exceptions are only authorised by the Chief Information Security Officer..

a. Users or 3rd Parties (where applicable) have the responsibility to report the following to StAH management:
   i. Asset misuse
   ii. Loss or theft of an asset
   iii. Unauthorised disclosure of information or data
   iv. Accidental disclosure of information or data

b. A non-exhaustive list of those activities considered unacceptable within StAH as follows:
   i. Unauthorised reproduction of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited.
   ii. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Senior Information Risk Owner (SIRO) should be consulted prior to the export of any material that is in question.
   iii. Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
   iv. Making fraudulent offers of products, items, or services originating from any account.
   v. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
   vi. Providing information about, or lists of, employees to parties outside of StAH.
   vii. Accessing data, a device or an account, for any purpose other than conducting business, or that aligns with approved reasonable personal use, even if you have authorised access, is prohibited.
   viii. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by StAH, is prohibited.
   ix. Under no circumstances is an employee of StAH authorised to engage in any activity that is illegal under UK or international law while utilising StAH owned/leased resources and assets.

c. All users must ensure all assets in their charge are returned upon termination of employment, or when they no longer require its use.

Reasonable Personal Use of StAH Assets

a. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. If there is any uncertainty, employees should consult their supervisor or manager. However, personal use should not negatively impact operational obligations at an individual or departmental level.

b. Reasonable personal use within StAH is defined as follows:
   i. Is lawful and ethical
   ii. Is in accordance with this, and all StAH Policy
   iii. Takes place during authorised breaks or outside of your working hours
   iv. Does not adversely affect your productivity
   v. Does not make unreasonable use of limited company resources
   vi. Does not facilitate personal gain i.e. financial reward
   vii. It does not harm the reputation of StAH

c. Those contracted as a 3rd Party must not use StAH assets for personal use.

d. Company data or information (with the exception of public data) must not be used for personal use.

Use of Mobile Devices in Patient Facing Areas

Overarching Principles

a. Mobile devices are not allowed on wards.

b. Mobile devices in patient facing areas must be secured with an alphanumerical and/or biometric password.

c. Users must ensure that other devices cannot connect to their mobile device or use its Wi-Fi capability (e.g. hotspots).

d. If a mobile device or related equipment is lost in a patient facing area it must be reported, at a minimum, to the following;
   i. Security Team
   ii. Site Co-ordinator
   iii. Line Manager
   iv. Raised as an incident on Datix

e. Mobile devices are permitted on Charity grounds and in Workbridge.

f. Users must not allow patients to have any access to their mobile device.

g. Personal mobile devices must not be used whilst involved in direct patient care.

h. Users must not use their personal mobile device to take photographs or video/audio clips in patient facing areas, or of patients and/or members of staff carrying out their duties.

i. Any breach of these requirements by a user may result in disciplinary action.

j. StAH is not responsible for the loss, theft or damage of a user's personal mobile device whilst on the Charity's premises.

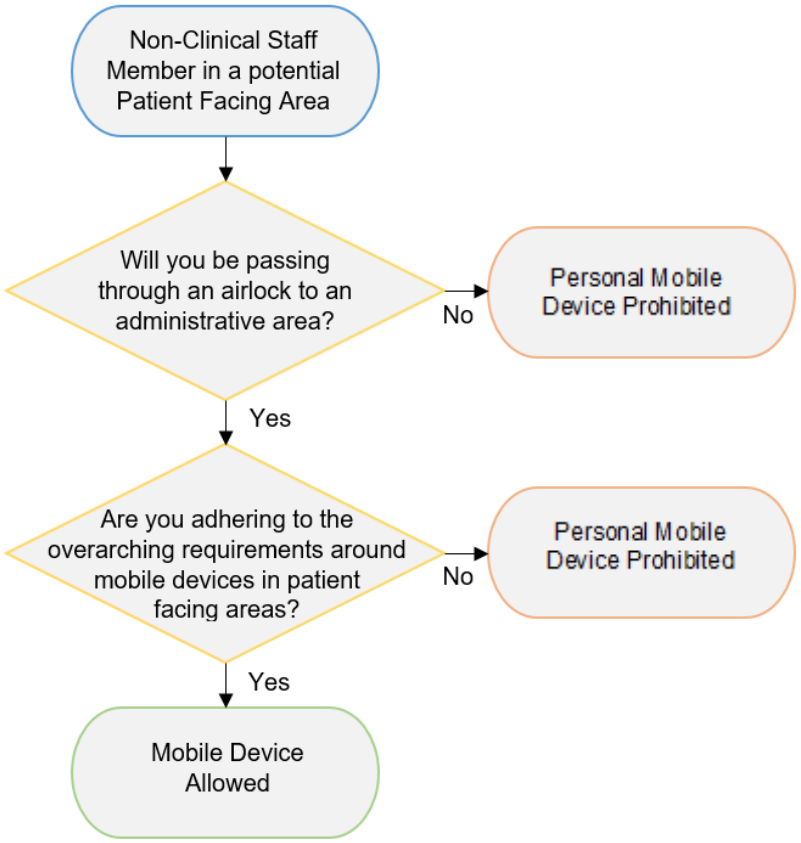
Specific Considerations

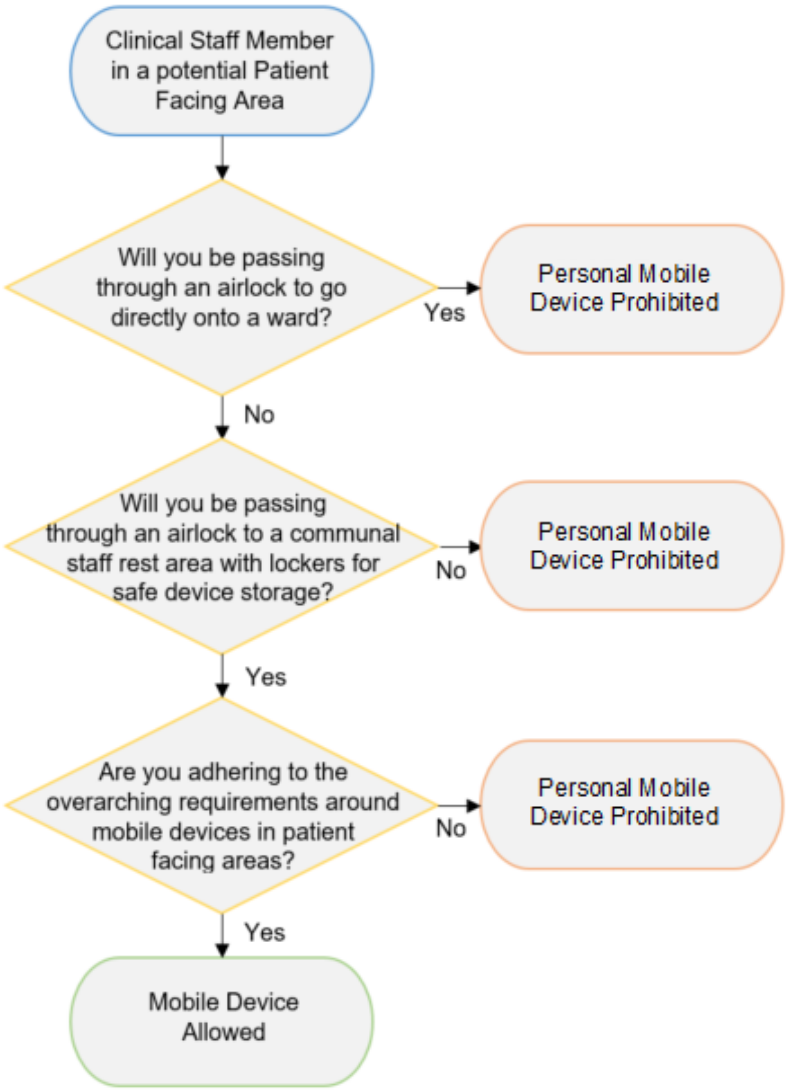
a. Mobile devices are permitted in the following circumstances, but must be used in accordance with the overarching principles outlined in the above section;
   i. Non-clinical staff passing through an airlock (potentially via a patient facing area) to an administrative area.

ii. An administrative area is an area not primarily utilised for direct patient contact e.g. top floor of William Wake House.

iii. Clinical staff passing through an airlock to a communal staff rest area with lockers where the device can be stored safely off a ward.

Flowcharts





Logging and Monitoring

a. Individuals working for or on behalf of StAH should not have an expectation of privacy whilst using the Charity's resources. All activities conducted either on a corporate or personal device using a StAH owned network/StAH O365 suite will be monitored to ensure these activities are appropriate and legal.

b. Staff member should be aware that some telephone call (mainly 2222 and 4422, which are utilised by the Estates Service Desk) might be recorded for training, awareness, and/or investigation purposes.

c. For more detail surrounding logging and monitoring requirements, please refer to StAH's Logging and Monitoring Standard.

E-Communications

a. Electronic communications (known as 'e-communications' for the purposes of this document), covered by this standard include, but are not limited to:

i. Email
ii. Microsoft Teams
iii. Telephone Communication
iv. Text/SMS messages
v. Any other digital messaging technologies/mediums

b. The following activities within e-communications are prohibited:
   i. Any form of harassment via e-communication
   ii. Mass distribution of emails to internal employees (unless there is a legitimate business requirement)
   iii. Unauthorised use of, or forging of email header information
   iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
   v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type
   vi. Forwarding of known phishing, toxic or suspicious emails to any email address other than phishing@stah.org
   vii. Use of unsolicited email originating from within networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by or connected via StAH's network
   viii. E-communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass co-workers or third parties; or disrupt the workplace
   ix. Transmitting offensive e-communications which contain, or promote Illegal, inappropriate material, including any material which may considered bullying, racist or degrading to an individual, ethnic group or religion.
   x. Impersonation of any other person in an email
   xi. Calling premium rate numbers or services
   xii. Excessive personal use
   xiii. International phone calls for personal use
   xiv. Use of non-StAH e-communication facilities to conduct StAH business i.e. personal emails or storage mediums.

Authentication Information

a. Secret Authentication information (credentials, passwords, security passes, keys etc.) must not be disclosed, shared, or put at risk of compromise.

b. Providing access to another individual, either deliberately or through failure to secure your authentication information is strictly prohibited.

c. Users are responsible for all activity performed with their StAH issued User IDs, and therefore will be held accountable for any misuse.

d. Users must not perform any activities with User IDs belonging to others, with the exception of shared or generic accounts via dispensation.

e. Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members when work is being done at home.

f. For more information towards the handling of authentication information, please refer to StAH's

Access Control Standard.

IT Equipment and Networks

a. The modification of accessibility, display and user interfaces is permitted providing they do not contravene this Standard

b. The following activities are prohibited:

   i. Modification to any security configurations i.e. encryption, anti-malware, monitoring, firewall and management applications

   ii. Port scanning or security scanning unless prior approval from Information Security has been obtained

   iii. Creating security breaches or intentionally/recklessly disrupting network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes

   iv. Circumventing user authentication or security of any host, network or account

   v. Introducing honeypots/nets or similar technology on the network

   vi. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)

   vii. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet

   viii. Use of web browsing facilities to access any material that is illegal, explicit, offensive, obscene, defamatory, abusive, and intimidating to others

   ix. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty

   x. Introducing malicious programs onto the network or network device (e.g., viruses, worms, Trojan horses, logic bombs, etc.)

3rd Party Software

a. Only approved 3rd party software can be introduced to the network. Approval must be sought from the Information Security team, Information Governance team, and the IT Service Manager.

b. Approved 3rd Party software must be used in accordance with the supplier's licensing and terms of use.

c. Any unapproved 3rd party software is prohibited.

Storage and Transmission of Information and Data

a. No unauthorised storage, carriage or transferral of StAH data or information is permitted. This includes the use of:

   i. Cloud storage (including the use of personal email to distribute StAH information) is strictly prohibited.

   ii. Removable media (Mass Storage, USBs, Flash Drives, and DVDs) is not permitted, unless approval is sought from the Information Security Team.

b. For the acceptable use and handling of data and information, please refer to StAH's Information Transfer Procedure, and StAH's Information Classification and Handling Procedure.

Office Working

Despite working within the secure boundaries of a StAH site, controls need to be implemented to mitigate the threat of unauthorised or malicious personnel. These controls are as follows:

a. All company information is to be secured appropriately at the end of the working day.

b. Physical assets such as laptops, mobile devices and approved USBs must be secured in a locked area at the end of the working day.

c. As a general rule, sensitive and confidential information should not be left unattended.

d. Printing:
   i. All printers/scanners must be clear of printer paper at the end of the working day
   ii. Users must authenticate for print/scanning services

e. If left unattended, computers must be 'locked' to ensure no one is able to access the device.

Remote and Mobile Working

There may be the requirement for users to work remotely e.g. public transport, hotel etc. The risks associated with remote working are considered greater as the utilised asset is not within the normal physical security boundaries found in the office. As such, special attention must be given to ensure all assets remain in view of the asset custodian and are not left unattended. Particular consideration should be given towards the following:

a. Public Transport / Locations
   i. Shoulder surfing or eavesdropping, whereby sensitive information may be visible or audible to unauthorised individuals is a significant risk. Therefore, attention must be paid to ensure information disclosure is minimised
   ii. Unattended assets are more susceptible to theft, and therefore should not be left unattended in any circumstances
   iii. The likelihood of forgetting assets is greater, so take particular care not to leave any information behind
   iv. StAH devices must not be taken abroad, unless authorisation has been granted by Information Governance.

b. Internet links / Wi-Fi Availability
   i. Most publicly available internet services (BT-Fon, Hotel Wireless etc.) are not as secure as corporate network. If there is a legitimate business requirement to access these services, ensure you are connecting to company resources via your VPN.

Home Working

a. StAH recognises that 'working from home' is fast becoming part of an employee's normal working routine. If approved by their line management, users should pay particular consideration towards the following:
   i. It is discouraged to store or process paper-based assets in a home environment
   ii. All efforts must be made to secure assets and dispose of them in accordance with Charity practices

iii. If left unattended, computers must be 'locked' to ensure no one is able to access the device

iv. The use of home printers is discouraged, if there is a business need to attach a printer for home working this must be approved by the Chief Information Security Officer..

v. Employees must only use a StAH provided laptop to access Charity information/applications or if using a personal device, access is only provided to Office 365.

vi. Laptops should only be used by an employee of StAH and not by any other family members, household dwellers or visitors.

vii. MFA should be enabled on all Laptops used offsite

b. Home Wi-Fi routers should be secured by ensuring that:

i. The default Wi-Fi password has been changed

ii. The password used to access and administer the router has been changed.

iii. The strongest encryption available is used i.e. 'WPA2'

iv. WPS has been disabled.

v. The router is set to automatically receive updates with the latest firmware as and when available.

c. For information referring to the use of USB storage devices, please refer to section 'Storage and Transmission of Information and Data'

d. Any unapproved hardware attached to a StAH laptop is prohibited owing to the risk of malware and inherent security vulnerabilities, unless specifically approved by the Chrief Information Security Officer..

BYOD

a. In order to be able to use personal devices to work with St Andrew's healthcare systems, users must ensure the following:

i. Devices should be secured with an alphanumerical and/or biometric password and according to the latest version of the Acceptable Use Standard.

ii. Passwords must be kept confidential and must not be shared with others.

iii. Devices should be configured so that they are automatically locked after being left idle for a period of time of no more than five minutes.

iv. Care must be taken to avoid actions that could pose a risk to confidentiality, whether by clicking on links on suspicious emails, accessing potentially harmful websites, using potentially harmful software application, using public Wi-Fi. Some apps may be capable of accessing sensitive information.

v. Mobile devices must not be 'Jailbroken' or 'rooted', or have otherwise circumvented the installed operating system security requirements.

vi. In the event that a device containing St Andrew's Healthcare data is lost or stolen, or is suspected of having been lost or stolen, IT must be informed as soon as possible so that appropriate measures may be taken to secure the compromised account.

vii. Information which is stored on the mobile device (including any removable storage) and is classed as Internal or above, must be protected via encryption.

viii. Approved anti-virus and anti-malware must be used and must be kept up to date. The latest security updates to the operating system and browsing software must be routinely installed.

ix. Public Wi-Fi networks may not be secure and should be avoided, unless using the St

Andrew's Healthcare Virtual Private Network (VPN).

x. If a device needs to be repaired, appropriate measures must be taken to ensure that St Andrew's Healthcare information cannot be seen or copied by the repairer.

xi. In the event that a device needs to be disposed of, IT Service Desk must be contacted to ensure any St Andrew's Healthcare information can be destroyed or wiped.

xii. In the event of the staff member leaving St Andrew's healthcare, appropriate measures must be taken by IT to remove St Andrew's Healthcare data from the device.

b. For more information regarding BYOD, see the StAH Bring Your Own Device Procedure.

Use of non-StAH Equipment on StAH Networks

a. StAH recognises the ever-increasing need for individuals to use personal devices (Laptops, Phones, tablet devices) to access the StAH O365 suite. The use of personal devices increases the risk of data loss/ compromise of data due to the security settings of the device not being controlled by StAH.

b. In order to mitigate the risks posed by using personal devices to access the StAH O365 suite, all such devices should be added, where possible, to the StAH mobile device management (MDM) tool.

c. Personal owned devices accessing the O365 suite that are not added to the MDM tool must be done so through a secure web browser session.

d. When accessing O365 from a personal device, the StAH MDM tool has a number of restrictions in place to minimise the risk of data loss from:

i. Downloading any information to a personal device.

ii. Taking screen shots of information using the personal device

iii. Downloading unapproved software to the device.

e. Lost/Stolen devices must be reported to the service desk immediately

f. The use of personal devices must be in accordance with this Acceptable Use standard.

Phishing

StAH accepts that email communications to and from external sources may form part of a user's daily working routine. As such, great care must be taken to ensure users remain vigilant to malicious, fraudulent and/or phishing emails. Users must therefore ensure the following:

a. The online 'Cyber Security Awareness' e-learning course on SAP has been completed as part of their mandatory training yearly

b. Be able to spot common phishing traits such as:

i. Bad grammar, formatting and spelling mistakes

ii. Promoting a sense of urgency, intrigue or consequence of non-action

iii. Strange email titles and senders' email addresses

iv. Suspicious links or attachments

v. Any unexpected content such as unpaid invoices, or any request relating to your IT account and password that you were not expecting to receive

c. Forward suspicious emails to the 'phishing@stah.org' mailbox or click on the 'Report

Phishing' icon and select the appropriate option.

d. Email Encryption and anto phishing software is installed on Stah systems to help minimise the risk to all users

e.

f. Ensure that any of the following conditions are immediately reported to the IT Service Desk on ext. 4444.

   i. Any interaction with a phishing link or attachment resulting in any unusual system behaviour such as pop-up boxes, strange notices anti-virus alerts or pages blocked by the web filter.

   ii. Any prompt to enter your username and password to release a file or view an attachment.

   iii. If you enter your username and password and submit this data resulting in an unexpected outcome.

g. Users must understand that they have an obligation to report any of the above conditions to ensure the IT Incident Response Team can take immediate action to investigate and respond to any potential compromise.

Social Media

a. StAH recognises and accepts that social media is being increasingly utilised for advertising, branding, recruitment, research, collaboration and also for personal use as a way of interacting socially with colleagues and friends. Whilst the Charity does not wish to discourage personnel from accessing such sites on the Internet, it does expect certain standards of conduct to be observed to protect both its legitimate business interests and its personnel from the dangers of inappropriate use. This applies both inside and outside the workplace and working hours.

b. StAH's Communications team should maintain a list of authorised communication channels, and forums and ensure the following:

   i. Individuals must obtain "approval to write/post" prior to any posting if relating to StAH or business information / practices

   ii. Social media accounts under the name of StAH must not be created without authorisation

   iii. If you are posting about St Andrew's or business information / practices on a regular basis (i.e. more than once a month), please inform and seek the guidance of the Communications Team and PR function.

   iv. Manage the credentials used to access shared social media sites, and ensure that those credentials are changed should they be exposed, or, known to an individual who is leaving the Charity, or Communications Team.

   v. Respect and abide by the rules, norms and guidelines of each online venue.

c. Prior to posting on social media, or other public forums the following must be considered:

   i. Information posted on social networks, blogs, message forums, etc., often becomes the property of that network once it has been submitted.

   ii. Care must be taken to properly structure comments and questions related to public postings on the Internet.

   iii. Consideration towards the content of the communications to ensure StAH is not placed at a competitive or other disadvantage or whether the material could cause public relations problems and or contravene confidentiality.

   iv. Personnel approved to use social media are bound by all StAH Policies.

d. Under no circumstance, inside or outside working hours, whilst using personal or StAH owned devices:

   i. Make reference to St Andrew's suppliers, customers, personnel or service users on social networking sites or blogs, unless authorised to do so

   ii. Make offensive, defamatory or inappropriate comments about St Andrew's, suppliers, customers, personnel or service users

   iii. Divulge confidential information about, or belonging to, St Andrew's, its suppliers, customers, personnel or service users on social networking sites or blogs unless authorised to do so

e. If you actively identify yourself as working for, or on behalf of StAH (e.g. LinkedIn) or are identifiable as StAH personnel, the following must be adhered to:

   i. Check your privacy settings on any social network sites and, where appropriate and possible, limit who has visibility of your profile

   ii. Check what kind of information you have visible, personal telephone numbers, email addresses, full birth dates across all sites to ensure information about you cannot be aggregated from multiple sources

   iii. Report any occurrences of individuals asking detailed questions regarding your place of work, current and past service users, current and past colleagues

   iv. Do not mix the professional and the personal in ways likely to bring the Charity into disrepute

   v. Post meaningful, respectful comments – in other words, no spam and no remarks that are off-topic or offensive

   vi. Do not imply St Andrew's endorsement of your personal views

   vii. Respect the confidentiality of StAH's data and information

   viii. When disagreeing with others' opinions, keep it appropriate and polite

   ix. If you're unsure of the sensitivity of a particular subject, or you notice potentially destructive posts, or literature about StAH, report it to your Line Manager.

f. Postings by employees from a StAH email address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of StAH, unless posting is in the course of business duties.

g. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by StAH's Data Protection Policy when engaged in blogging.

h. When engaged in blogging, employees must not attribute personal statements, opinions or beliefs to StAH, when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of StAH. Employees assume any and all risk associated with blogging.

i. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of and/or any of its employees. Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments or otherwise engaging in any conduct prohibited by StAH's Code of Conduct.

j. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, StAH's trademarks, logos and any other intellectual property must not be used in connection with any blogging activity

Guest Wi-Fi

a. This guest network is the property of St Andrew's Healthcare and is for use by authorised 3rd parties only, and not for general use for St Andrew's employees.

b. By using our guest internet service, you hereby expressly acknowledge and agree that there are significant security, privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology. Security issues include, without limitation, interception of transmissions, loss of data, and the introduction or viruses and other programs that can corrupt or damage your computer.

c. You agree that the owner and/or provider of this network is NOT liable for any interception or transmissions, computer worms or viruses, loss of data, file corruption, hacking or damage to your computer or other devices that result from the transmission or download of information or materials through the internet service provided.

d. Use of the wireless network is subject to the general restrictions outlined below. If abnormal, illegal, or unauthorised behaviour is detected, including heavy consumption of bandwidth, the network provider reserves the right to permanently disconnect the offending device from the wireless network.

e. The following examples of Unacceptable Uses are representative examples only and do not comprise a comprehensive list of unacceptable uses:

   i. Accessing illegal material, or conducting illegal activities

   ii. High bandwidth operations, such as large file transfers and media sharing with peer-to-peer programs (i.e.torrents)

   iii. Obscene or indecent speech or materials

   iv. Defamatory or abusive language

   v. Using the Service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.

   vi. Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

   vii. Facilitating a Violation of these Terms of Use

   viii. Distribution of Internet viruses, Trojan horses, or other destructive activities

   ix. Distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the node or any connected network, system, service, or equipment.

   x. Advertising, transmitting, or otherwise making available any software product, product, or service that is designed to violate these Terms of Use, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail-bombing, denial of service attacks, and piracy of software.

   xi. The sale, transfer, or rental of the Service to customers, clients or other third parties, either directly or as part of a service or product created for resale.

   xii. Seeking information on passwords or data belonging to another user.

   xiii. Making unauthorised copies of proprietary software or offering unauthorised copies of proprietary software to others.

   xiv. Intercepting or examining the content of messages, files or communications in transit on a data network.

f. Any use of this service, may be intercepted, monitored, recorded and audited. Unauthorised or improper usage of this service, data or information may result in disciplinary action, sanction for third parties and/or criminal proceedings.

Prohibited Material

a. Access to, or distribution and storing of the following material is prohibited:

   i. Pornographic Material, irrespective of grade or category
   ii. Material which may be considered offensive, or intrusive
   iii. Militant or Extremist Material which also may incite racism or terrorism

Audit and Compliance

a. The Information Security Team will perform regular audits to ensure policy compliance as per the ISMS Audit Schedule. Any non-compliance will be reported and managed via the non-conformance process.

b. Any exceptions to this standard will be managed via the dispensation process.

c. All members of staff are responsible for reporting confirmed or suspected breaches of this standard to the IT Service Desk.

d. A member of staff found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

Monitoring and oversight

a. The Chief Information Security Officer is responsible for ensuring this document remains fit for purpose and up to date.