POLICY TITLE:	**IT Security**
Policy Number:	AIT02
Applies to:	All Aspris Services
Version Number:	01
Date of Issue:	20/10/2021
Date of Review:	01/09/2024
Author:	IT Department
Ratified by:	Brian McCallion, IT Risk & Compliance Manager
Responsible signatory:	Clair Dunn, IT Director
Outcome:	This Policy: • Details colleagues' responsibilities for computer security within Aspris, and is designed to help them understand their position. • Sets out colleagues' responsibilities for computer security for additional services that a user may have over and above a basic user.
Cross Reference:	ALE03 Data Protection ALE06 Confidentiality AOP50 Driving at Work AHR04.10 Anti-Bullying and Harassment AHR06 Termination of Employment (Leavers) AHR11 Use of Social Media by Colleagues AIT10 Information Asset Management AIT11 Information Transfers AIT12 Use your Aspris or Personal Mobile Device

EQUALITY AND DIVERSITY STATEMENT

Aspris is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics and all will be treated with dignity and respect

This policy cover all parts of Aspris Services – The Care and Education Divisions; Central services and our Fostering service. For the Fostering service and the 2 operational divisions, there are local procedures that relate to some of these policies, where necessary.

In order to ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, email AsprisGovernanceHelpdesk@Aspris.com.

IT SECURITY

Contents **Page**

1 VERSION CONTROL

1.1

Issue No.	Comments	Updated	Date
V01	Introduction of new policies for Aspris	IT Department	01/09/2021

2 INTRODUCTION

2.1 Aspris depends on its computers, data, information processing capabilities and telecommunications systems for our day to day business. IT systems are a critical part of our information infrastructure. It is vitally important, therefore, that the security of these systems and the data held by Aspris is maintained. Sections 5 & 6 within this IT Security Policy detail Colleagues' and Line Managers' responsibilities for computer security and are designed to help you to understand your role. Compliance with this policy is part of your contract of employment with Aspris. Any breach could lead to disciplinary action being taken against you, which in turn could lead to the termination of your employment. You should therefore take the time to read and understand this. If there are any queries with regard to this document, please feel free to contact a member of the Aspris IT Helpdesk, for clarification.

Thank you for your cooperation.
Tina Walton, Chief Services Officer
Clair Dunn, IT Director

Dated: September 2021

3 SCOPE

3.1 The policy applies to all colleagues, contractors, temporary and other workers within Aspris, referred to as 'colleagues' within this document, who have been provided with access to Aspris IT Services.

3.2 It applies to:

(a) Any servers, personal computers, mobile devices, remote access facilities, outside suppliers of data, LANs (Local Area Networks), WANS (Wide Area Networks), and communication systems
(b) All software used on Aspris computer systems, whether packaged or bespoke and third party software provided as a software as a service accessed through a public network
(c) All information and reports created using Aspris data
(d) All programs developed in Aspris time, using Aspris equipment, or by colleagues
(e) All computers, communications links, and associated equipment at services or central services locations or connected to Aspris computers.

3.3 Note that the use of Aspris IT equipment by children and young people is restricted to specifically designated equipment at services connected to Aspris IT Services. Third parties are not permitted to use or plug-in to any Aspris IT equipment.

4 RESPONSIBILITIES

4.1 **The IT Director** has overall responsibility for ensuring that Aspris has adequate computer security measures in place.

4.1.1 IT security and information risks must be identified and addressed in every project and dealt with in accordance with the IT Departments MC17 Risk Management in Projects departmental procedure.

4.2 **Colleagues' Responsibilities -** every colleague is responsible for the protection of our assets, including computers and data. Colleagues should notify their Line Manager or Aspris IT Helpdesk immediately whenever he or she sees actions that go against, or seem to go against, this policy.

4.2.1 As a colleague you are responsible for adhering to this policy when undertaking your role.

4.2.2 IT equipment or data shall not be removed from a service or central services location unless it is a requirement of your job role or you have been provided with written authorisation by the service leader / central services team leader.

4.2.3 If you have access to personal data such as salaries, home telephone numbers, children and young people's information etc., you must at all times, adhere to the provisions of the Data Protection Act 2018. In particular, you must ensure they comply with the Act when transferring or disclosing any data or information to external organisations. (See ALE03 Data Protection, ALE06 Confidentiality and AIT11 Information Transfers).

4.2.4 You shall use Aspris IT Services only for authorised purposes. To use Aspris IT Services for other purposes may be an offence under the Computer Misuse Act 1990. In particular no colleagues are authorised to install software on any Aspris computer without approval of the IT Department.

4.2.5 It is your responsibility to ensure that all computers used during the day are logged out and closed down in a controlled manner, before leaving the service or central services location. Unattended computers that are left logged on constitute a serious security risk, and can be interpreted as a misuse of the Aspris IT Services.

4.2.6 You must ensure that security is maintained at all times by locking your computer when it is left unattended; for example, during lunch time, when attending meetings, or when temporarily leaving the site.

4.2.7 You are responsible for the security and integrity of information stored on your computer. This responsibility includes making regular backups of any data held on local drives.

4.2.8 You are responsible for the physical security of equipment such as laptop computers and mobile phones that are issued to you. You must take sensible and reasonable precautions to ensure that your equipment is not lost or stolen by not leaving it unattended or left unsecured in an unsafe place. Mobile devices should be secured or locked away when left unattended. Additional care and vigilance is required when using equipment in public places, carried on public transport or transported by car.

4.2.9 You are responsible for the security of any passwords or PINs issued to you for the purposes of accessing Aspris IT and telecommunications systems including computers and mobile phones. In particular, such passwords and PINs must not be disclosed to anyone and not shared with other colleagues (with the exception of IT Department – See Section 18 IT Support). You must not solicit the disclosure of a password or PIN from another colleague.

4.2.10 You should be aware of the potential for fraud arising from social engineering attacks e.g. phishing and vishing, the use of scanned signatures and should therefore be careful with their storage, use and dissemination.

4.3 **Line Managers** have responsibility for distribution and application of this policy and shall ensure:

(a) Every colleague is provided with a copy of this policy at recruitment and updates thereafter

(b) **IT Department are informed** of every colleague who has access to Aspris IT services, when they **transfer sites/teams, change roles or they no longer work for the Aspris**, in order to adjust computer access privileges as needed

(c) When a colleague's contract is terminated for any reason, you are responsible for ensuring the colleague's computer privileges are revoked at once on all computer systems. You are responsible for notifying the IT Department when a user's access should be revoked or deleted. Refer to AHR4.06 Termination of Employment (Leavers)

(d) You are responsible for the safe return to IT Department of any IT information assets utilised by any departing colleagues, including laptop computers, removable media, printers, mobile phones and communications equipment and electronic and paper documents. Refer to AHR4.06 Termination of Employment (Leavers).

All colleagues shall comply with this policy at all times and any contravention could be classed as a disciplinary offence which may result in the disciplinary action and termination of employment.

5 EMAIL USAGE

5.1 If an email is sent originating from Aspris, the general public will tend to view that message as an official policy statement. This document sets out the policy for the protection of confidentiality, integrity and availability of email systems within Aspris, to prevent tarnishing the public image of Aspris.

5.2 This section covers appropriate use of any email sent from an Aspris email address and applies to all colleagues, contractors, consultants, temporary and other workers within Aspris.

5.3 **Prohibited Use:**

(a) The Aspris email system shall not be used to send or forward emails or documents containing libellous, harassing or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography,

religious beliefs and practice, political beliefs, or national origin. Colleagues who receive any emails with this content from any colleague should report the matter to their line manager immediately

(b) Users must not send unsolicited email messages, forge or attempt to forge email messages, send emails using another user's email account
(c) Sending chain letters or joke emails from an Aspris email account is prohibited
(d) Users must not breach copyright or licensing laws when composing emails or email attachments
(e) These restrictions also apply to the forwarding of mail received from a colleague
(f) Virus or other malware warnings and mass mailings sent to colleagues shall be approved by the IT Department before sending.

5.3.1 **Confidential Information -** Email is not a secure system. Confidential information should not be sent by email to an external email address unless it has been encrypted using the Outlook O365 Message encryption option. Due to the security controls in place within the Aspris email system, emails sent to internal email accounts can contain confidential information, but the sender has the responsibility to check that the recipient has a legitimate requirement to see the confidential information. **NB:** Information received internally containing confidential information must not be sent to an external email address. Extra care must be taken when forwarding an 'email trail' or attachments to an external email address, to make sure that no confidential information is contained within the trail or the attachments.

5.3.2 **Personal Use -** Using a reasonable amount of Aspris resources for personal emails is acceptable, but should not interfere with your work. Personal emails should adhere to all the guidance in this policy. Personal emails shall be saved in a separate folder from work related email and be deleted on a weekly basis.

5.3.3 **Monitoring -** Users should be aware that email sent or received via Aspris IT Services may be intercepted and monitored for a variety of purposes, including, but not limited to, ensuring compliance with internal policies, supporting internal investigations, assisting with the management of Aspris IT Services and in support of Aspris business.

5.3.4 **Storage/Retention** - In accordance with the company retention policy, the email system is not considered to be a permanent data store. Users shall ensure that emails and/or attachments that need to be retained should be saved to an appropriate destination folder within a shared drive or application that the user has access to. Users should be conscious that any file saved to a shared drive will be accessible to anyone with permission to that file store unless permission restrictions have been applied to the destination folder by IT.

6 PASSWORD CONTROL

6.1 **Overview -** Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Aspris IT Services. As such, all colleagues (including contractors and vendors with access to Aspris systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

6.2 This section covers the standards for creation of strong passwords, the protection of those passwords, and the frequency of change. It is applicable to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Aspris site, for access to the Aspris IT Services, for access to an Aspris application hosted as a software as a service or stores any non-public Aspris information.

6.3 **General**

(a) No one is to be permitted to use Aspris computers without an approved user account
(b) To obtain a user account requires the approval of your line manager

(c) Each user is responsible for all activity that occurs on any system where access is provisioned through the use of their user account
(d) User accounts may be revoked (or deleted or disabled) at any time through the agreement of the Chief Services Officer
(e) A User account will be revoked when a colleague terminates employment
(f) All system-level passwords (e.g. server admin, application administration accounts, etc.) must be changed every 365 days
(g) User-level passwords (e.g., Aspris IT Services access, application access etc.) are set by Aspris Policy to be changed every 365 days
(h) Passwords must be memorised and never written down, saved within browsers or inserted into email messages or other forms of electronic communication
(i) Passwords should never be shared with anyone else (with the exception of the IT Department – See Section 18 IT Support).
(j) All user-level and system-level passwords must conform to the guidelines described below.

6.4 **Password Construction Guidelines -** Passwords are used for various purposes within Aspris. Some of the more common uses include: user level accounts, application accounts, email accounts. Everyone should be aware of how to create a strong password.

6.4.1 Poor, weak passwords have the following characteristics unless supported by two factor authentication:
(a) The password contains less than fifteen characters
(b) The password is a word found in a dictionary (English or foreign)
(c) The password is a common usage word such as:
  i. Names of family, pets, friends, co-workers, fantasy characters, etc; computer terms and names, commands, sites, companies, hardware, software; the words "Aspris", or any derivation
  ii. Birthdays and other personal information such as addresses and phone numbers
  iii. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  iv. Any of the above spelled backwards
  v. Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

6.4.2 Within Aspris, strong passwords shall have the following characteristics, where two factor authentication and single sign-on has been implemented:
(a) Contain both upper and lower case characters (e.g. a-z, A-Z)
(b) Have digits and punctuation characters as well as letters e.g. 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
(c) Are at least eight alphanumeric characters long
(d) Are not a word in any language, slang, dialect, jargon, etc.
(e) Are not based on personal information, names of family, etc.
(f) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "This.may.B1w2R!" or some other variation.

6.5 **Password Protection Standards -** Do not use the same password for Aspris accounts as for other non-Aspris access (e.g. personal email account, online banking, etc.). Don't use the same password across all the systems you access. For example, select one password for Aspris IT Services and separate passwords for other IT applications not accessed through single-sign-on. Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Aspris information. Here is a list of 'dont's':
(a) Don't reveal a password over the phone to ANYONE (with the exception of IT Department – See Section 18 IT Support)
(b) Don't reveal a password in an email message
(c) Don't reveal a password to your line manager

(d) Don't talk about a password in front of others
(e) Don't hint at the format of a password (e.g. "my family name")
(f) Don't reveal a password on questionnaires or security forms
(g) Don't share a password with family members
(h) Don't reveal a password to your colleagues whilst on holiday
(i) Don't use the "Remember Password" feature in browsers
(j) Don't write passwords down and store them anywhere. Do not store passwords in a file stored within Aspris IT Services.

6.5.1 If someone demands a password (with the exception of IT Department – See Section 18 IT Support), refer them to this document or have them call someone in the IT Department, and if an account or password is suspected to have been compromised, immediately report the incident to the IT Department and change all your passwords.

7 COMPUTER SECURITY (CLEAR DESK AND CLEAR SCREEN POLICY)

7.1 The purpose of this section is to provide guidance for computer security to ensure the security of information on the computers and information the computers may have access to. It applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties with an Aspris workstation connected to Aspris IT Services.

7.2 Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of confidential information and that access to confidential information is restricted to authorised users.

7.3 Colleagues using computers shall consider the confidentiality of the information that may be accessed and minimise the possibility of unauthorised access.

7.4 Aspris will implement physical and technical safeguards for all computers that access electronic sensitive information to restrict access to authorised users.

7.5 Appropriate measures include:
(a) Restricting physical access to computers to only authorised personnel
(b) Securing computers (screen lock or logout) prior to leaving area to prevent unauthorised access. As an additional safeguard computers will be set to autolock after 15 minutes inactivity
(c) Complying with all applicable password policies and procedures
(d) Ensuring computers are used for authorised business purposes only
(e) Never installing unauthorised software on computers
(f) Storing all confidential information on Aspris IT Services file stores
(g) Keeping food and drink away from computers in order to avoid accidental spills
(h) Securing laptops that contain confidential information by using cable locks or locking laptops up in drawers or cabinets to protect them from unauthorised access or theft
(i) Complying with the virus protection policy (see Section 8 Virus Protection)
(j) Ensuring that monitors are positioned away from public view (line of sight). If necessary, install privacy screen filters or other physical barriers to public viewing of monitors
(k) Ensuring that all computers are locked when unattended and turned off at the end of the working day
(l) If wireless network access is used, ensure access is secure by following the wireless communications policy (see Section 10 Wireless Communications (Wi-Fi)
(m) Any information assets including paper documents are removed from desks and locked away at the end of the working day.

8 VIRUS PROTECTION

8.1 Aspris must ensure that it protects its computer systems from external attacks. Aspris has a responsibility to protect the business from malware threats, such as viruses and spyware

applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

8.2 This section outlines the processes that colleagues can take to prevent virus problems and is applicable to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties who have access to Aspris IT Services.

8.3 It is the responsibility of the IT Department to ensure that antivirus software is installed, updated and managed correctly. All email messages and attachments are virus checked automatically by the email software. To further reduce the risk of virus attacks colleagues must:

(a) Not use any removeable media including, but not limited to; USB memory sticks, External Hard Drives or SD cards that have been used outside Aspris; in any Aspris equipment that is connected, or may be connected, to Aspris IT Services, without the prior approval of the IT Director
(b) Not allow the connection of any non-Aspris computer equipment to Aspris IT Services without the prior approval of the IT Director. If such permission is granted, the equipment must be checked for viruses by a member of the Aspris IT Helpdesk before a connection takes place
(c) Contact the Aspris IT Helpdesk immediately if there is any suspicion of a virus on their computer equipment. They must stop using the equipment immediately until given clearance by the Aspris IT Helpdesk
(d) Users should be aware that many hoax virus warnings exist. If any warning is received it should be sent to the Aspris IT Help Desk where its authenticity will be checked. Such warnings must not be forwarded to other colleagues
(e) Never click any links, open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your deleted items
(f) Delete spam, chain, and other junk email without forwarding to colleagues, in line with Section 9 Acceptable Use
(g) Never download files from unknown or suspicious sources
(h) Back-up critical data and system configurations on a regular basis and store the data on Aspris IT Services

9 ACCEPTABLE USE

9.1 The IT Department's intentions for publishing rules on the acceptable use of computer equipment are not to impose restrictions that are contrary to the Aspris established culture of openness, trust and integrity. The IT Department is committed to protecting colleagues and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

9.1.1 Aspris IT Services, including, but not limited to, computer equipment, software, operating systems, applications, storage media, accounts providing electronic mail, internet access and FTP, are the property of Aspris. These systems are to be used for business purposes in serving the interests of the company, and our children and young people in the course of normal operations.

9.1.2 Effective security is a team effort involving the participation and support of every colleague who deals with information and/or information systems. It is the responsibility of every colleague to know these guidelines, and to conduct their activities accordingly.

9.2 The purpose of this section is to outline the acceptable use of IT equipment and systems throughout Aspris. These rules are in place to protect colleagues and Aspris. Inappropriate use exposes Aspris to risks including virus attacks, compromise of Aspris IT Services, and legal issues.

9.3 This section applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Aspris.

9.4 **General Use and Ownership**

(a) While Aspris IT Services administration desires to provide a reasonable level of privacy, colleagues should be aware that the data they create on Aspris IT Services or associated systems remains the property of Aspris.

(b) Colleagues are responsible for exercising good judgement regarding reasonable personal use. Services and central services teams are responsible for creating guidelines concerning personal use of email/Internet/Intranet systems. In the absence of such policies, colleagues should be guided by services and central services teams procedures on personal use, and if there is any uncertainty, colleagues should consult their line manager

(c) IT Department recommends that any information that colleagues consider confidential be encrypted. For guidelines on information classification, see AIT10 Information Asset Management

(d) For security and maintenance purposes, authorised individuals within Aspris may monitor equipment and Aspris IT Services at any time

(e) Aspris reserves the right to audit Aspris IT Services on a periodic basis to ensure compliance with this policy.

9.4.1 **Security and Proprietary Information**

(a) Information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential, internal or public, as defined by the Information Classification section of this document (See Section 15 Information Classification). Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Colleagues should take all necessary steps to prevent unauthorised access to this information

(b) Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. Passwords should be changed every 365 days

(c) All computers should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by locking the computer (control-alt-delete / lock) when left unattended

(d) Because information contained on laptops and mobile phones is especially vulnerable, special care should be exercised when such equipment is being used in a public place, carried on public transport or transported by car

(e) Postings by colleagues from an Aspris email address to newsGroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Aspris, unless posting is in the course of business duties

(f) All computers used by the colleague that are connected to the Aspris Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database

(g) Colleagues must use extreme caution when opening email attachments received from unknown senders, which may contain malware, ransomware, viruses, email bombs, or Trojan horse code

(h) Colleagues should be on their guard against phishing attacks. Phishing is the act of sending an email to a user falsely claiming to be from a trustworthy source in an attempt to trick the user into surrendering confidential information. The phisher manipulates the sender's details to make it appear that it has come from someone else. Emails purporting to be sent from IT administrators are commonly used. Types of information that they try to obtain includes usernames, passwords and confidential information about an individual which can then be used for identity theft or some other financial gain. Some emails may simply ask you to reply with the information or complete and return an attachment. However, more sophisticated emails will contain web links that direct users to enter details at a fake website whose appearance is almost identical to the legitimate one.

9.4.2 **Unacceptable Use** - The following activities are, prohibited. However, colleagues may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration colleagues may have a need to disable the Aspris IT Services access of a computer if that computer is disrupting production services). Under no circumstances is a colleague authorised to engage in any activity that is illegal under English or international law while utilising Aspris-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

9.4.2.1 **Aspris IT Services Activities** - The following activities are **strictly prohibited**, with no exceptions:

(a) 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 Aspris
(b) Unauthorised copying 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 Aspris or the end user does not have an active license, is strictly prohibited
(c) Introduction of malicious programs into the Aspris IT Services (e.g. viruses, ransomware, etc.)
(d) Revealing your account password to others (with the exception of IT Department – See Section 18 IT Support). or allowing its use of your account by others. This includes family and other household members when work is being done at home
(e) Using an Aspris computing asset to actively engage in procuring or transmitting material that is in violation of AHR04.10 Anti-Bullying and Harassment
(f) Making fraudulent offers of products or services originating from any Aspris account
(g) Making statements about warranty, expressly or implied, unless it is a part of normal job duties
(h) Effecting security breaches or disruptions of Aspris IT Services. Security breaches include, but are not limited to, accessing data of which the colleague is not an intended recipient or logging into a server or account that the colleague 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, sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
(i) Port scanning or security scanning is expressly prohibited unless prior notification to the IT Department is made
(j) Executing any form of monitoring which will intercept data not intended for the colleague's computer, unless this activity is a part of the colleague's normal job/duty
(k) Circumventing user authentication or security of any computer or Aspris IT Services account
(l) Interfering with or denying service to any user other than the colleague's computer (for example, denial of service attack)
(m) 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
(n) Providing information about, or lists of, children and young people or colleagues to parties outside Aspris
(o) Aspris colleagues and contractors must not use non-Aspris PC's to undertake Aspris work activities or connect it or other unapproved device to Aspris IT Services
(p) Transferring company information to/from a personal computing device via email or storage device to facilitate Aspris work activities.

9.4.2.2 **Email and Communications Activities** - The following activities are **strictly prohibited**, with no exceptions:

(a) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam)
(b) Any form of harassment via email, telephone or text message, whether through language, frequency, or size of messages
(c) Unauthorised use, or forging, of email header information
(d) 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
(e) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type
(f) Use of unsolicited email originating from within Aspris IT Services or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Aspris or connected via Aspris IT Services
(g) Posting the same or similar non-business-related messages to large numbers of Usenet newsGroups (newsGroup spam)
(h) Colleagues and contractors must not use non-Aspris email accounts or other external resources to receive or send any communication or document in connection with Aspris business, thereby ensuring that official business is never confused with personal business. The only exception to this is with the express permission from the IT Director.

9.4.2.3 **Blogs, Forums and Social Networking Sites –**

(a) Data Protection requirements also applies to Blogging, Forums and Social Network postings. As such, colleagues are prohibited from revealing any Aspris confidential including information about our service users or proprietary information, trade secrets or any other material that would be covered by ALE03 Data Protection
(b) Colleagues shall not engage in any posting that may harm or tarnish the image, reputation and/or goodwill of the Aspris and/or any of its colleagues. Colleagues are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by AHR4.10 Anti Bullying and Harassment
(c) Colleagues may also not attribute personal statements, opinions or beliefs to the Aspris when engaged in these activities. If a colleague is expressing his or her beliefs and/or opinions, the colleague may not, expressly or implicitly, represent themselves as a colleague or representative of Aspris or any company within it. Colleagues assume any and all risk associated with posting on these sites
(d) Apart from following all laws pertaining to the handling and disclosure of copyrighted materials, Aspris trademarks, logos and any other Aspris intellectual property may also not be used in connection with any of these activities
(e) For further information on your employment responsibilities when engaging in these activities please refer to AHR11 Use of Social Media by Colleagues.

10 WIRELESS COMMUNICATIONS (Wi-Fi)

10.1 The purpose of this section is to ensure that Aspris secures and protects its information assets. Aspris provides computers, networks, and other electronic information systems to meet missions, goals, and initiatives. Aspris grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

10.1.1 This section specifies the conditions that Wi-Fi infrastructure devices must satisfy to connect to Aspris IT Services. Only those Wi-Fi infrastructure devices that meet the standards specified in this policy or are granted an exception by the IT Department are approved for connectivity to Aspris IT Services, and applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties that have a wireless infrastructure device issued by Aspris.

10.1.2 This is also applicable to all Wi-Fi infrastructure devices that connect to Aspris IT Services or reside at a service that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, tablets and smart phones. This includes any form of wireless

communication device capable of transmitting packet data. **The IT Department must approve exceptions to this in advance.**

10.2 **General Network Access Requirements** - All Wi-Fi infrastructure devices that reside at a site and connect to Aspris IT Services, or provide access to information classified as Internal or Confidential must:

(a) Abide by the standards specified in the Wireless Communication Standards
(b) Be installed, supported, and maintained by IT Department
(c) Use the Aspris approved authentication protocols and infrastructure
(d) Use the Aspris approved encryption protocols
(e) Maintain a hardware address (MAC address) that can be registered and tracked
(f) Not interfere with wireless access deployments maintained by other support organisations.

10.3 **Home Wireless Device Requirements** - Wireless infrastructure devices that provide direct access to Aspris IT Services, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standards.

10.3.1 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to Aspris IT Services. Access to Aspris IT Services through this device must use standard remote access authentication.

11 INTERNET ACCESS

11.1 The standards set out in this section are designed to minimise the potential risk to Aspris from damages which may result from unauthorised use of copyrighted material or damage to Aspris IT Services, due to malware infections.

11.2 This section applies to all colleagues, contractors, temporary and other workers at Aspris, including all personnel affiliated with third parties issued with a user account using an Aspris computer used to connect to Aspris IT Services who have been provided with access to the Internet.

11.3 **Acceptable Use -** Access to the internet is strictly limited and should be used for business use to access research material and other information relevant to Aspris work only. Colleagues may access websites for personal use so long as it does not interfere with their work or the availability and speed of Aspris IT Services. Personal use of the Internet must comply with this policy.

11.4 **Unacceptable Use:**

(a) Creating, downloading, uploading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material, or any data capable of being resolved into obscene images or material
(b) Creating, downloading or transmitting (other than for properly authorised and lawful research) any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material
(c) Creating, downloading or transmitting material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety or offence to people
(d) Creating or transmitting 'junk-mail' or 'Spam'. This means unsolicited commercial webmail, chain letters or advertisements
(e) Using the internet to conduct private freelance business for the purpose of commercial gain
(f) Downloading and use of streaming video or audio for entertainment purposes
(g) Downloading of any software – 'copyrighted' or otherwise
(h) Uploading or transmitting any company information or data not classified as public

(i) The downloading of music, audio or video files from the Internet is not permitted without the authority of the IT Director. In particular, the downloading of music, video or other media that is subject to copyright.

11.5 **Monitoring:**

(a) Access to the Internet is regulated centrally via a third party provider, to ensure that inappropriate and inoffensive sites cannot be accessed. Internet sites are blocked using a set of standard phrases, words or images which may cause offence or be detrimental to those that view them. Colleagues can make a request for a specific site to be blocked or unblocked (where a business or educational need exists) by contacting the IT Department

(b) Bitdefender internet site safeguards are deployed to disallow access to sites or downloads which are deemed to be unsafe.

(c) The IT Department monitors internet access for inappropriate use and will report any instances to senior management for appropriate disciplinary action.

12 SOFTWARE AND APP INSTALLATION

12.1 Allowing colleagues to install software and apps on servers, computers and mobile devices opens the organisation up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered in an audit, and programs which can be used to hack the organisation's computer systems are examples of the problems that can be introduced when colleagues install software on computing equipment.

12.2 The purpose of this section is to minimise the risk of loss of program functionality, the exposure of confidential information contained within Aspris IT Services, the risk of introducing malware, and the legal exposure of running unlicensed software and it applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties who use desktops, laptops, servers, smartphones and other computing devices operating within Aspris.

12.3 Colleagues shall not install software on Aspris computing devices. Software requests must first be approved by the colleagues Line Manager and sent to the Aspris IT Helpdesk via a Heat request or email. Software requested will be reviewed against an approved software list, maintained by the Aspris IT Helpdesk. Where the software is not on the approved list and software risk assessment will be performed by the IT Security Team. The IT Department will obtain and track the licenses, check new software for vulnerabilities, conflict and compatibility, and perform the installation when use is approved.

13 REMOVABLE MEDIA DEVICES

13.1 Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations. The purpose of this section is to minimise the risk of loss or exposure of sensitive information maintained by Aspris and to reduce the risk of acquiring malware infections on computers used by Aspris.

13.2 This section covers all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties when using all computers and servers operating within Aspris.

13.3 Aspris colleagues may use removable media in their computers on a read only basis. The security policy will stop items being removed or saved from Aspris IT Services and virus check files.

13.4 Only approved encrypted removable media devices approved and issued by the IT Department may be used to save or transfer information.

13.5 Confidential information should only be stored on removable media only when required in the performance of your assigned duties.

14 ACCEPTABLE ENCRYPTION

14.1 The purpose of this section is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this section provides direction to ensure that UK regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the UK. This section applies to all colleagues, contractors, temporary and other workers at the Aspris, including all personnel affiliated with third parties.

14.2 Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least AES 256-bit algorithm. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Aspris's key length requirements will be reviewed annually and upgraded as technology allows.

14.2.1 The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IT Department. Residents of countries other than the United Kingdom should make themselves aware of the encryption technology laws of the country in which they reside.

14.3 To protect information assets the following controls have been selected:
(a) Computers, Laptops and tablets issued to individual colleagues are encrypted
(b) External harddrives and USB data sticks used for storing non-public information assets are encrypted
(c) iPads and iPhones have password protection which encrypts the device when locked
(d) Smartphone devices have password protection
(e) iPad, iPhones and Smartphone devices have been enabled to allow the devices to be remotely wiped
(f) Remote access to the is secured using SSL sessions
(g) Websites and Software as a service are protected using secure sessions under https.

15 INFORMATION CLASSIFICATION

15.1 This section is intended to help colleagues determine what information can be disclosed to third parties, as well as the relative sensitivity of information that should not be disclosed outside of Aspris without proper authorisation.

15.1.1 The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

15.1.2 All colleagues should familiarise themselves with the information labelling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidance and to emphasise common sense steps that you can take to protect Aspris information (e.g. Aspris confidential information should not be left unattended in conference rooms).

15.1.3 Questions about the classification of a specific piece of information should be addressed to your line manager.

15.2 This section applies to colleagues, contractors, temporary and other workers at Aspris, including all personnel affiliated with third parties when accessing and using Aspris information. All Aspris information is categorised into three main classifications:
(a) Public
(b) Internal
(c) Confidential.

15.3 AIT10 Information Asset Management provides details of the classifications, how to protect information and who can be party to the information within Aspris.

15.4 AIT11 Information Transfers provides full details on how information must be transferred when being taken off-site or being sent electronically or by other media to a third party and who must approve it.

16 ACCESS TO DATA

16.1 Levels of access to data will be determined by service leaders and central services team leaders, in conjunction with the IT Director, who will ensure that levels of access are consistent throughout Aspris.

16.2 All users with access should ensure that all data is held on Aspris IT Services, which are backed up, nightly by the IT Department.

16.3 It is the responsibility of the user to protect any confidential data files against unauthorised reading and copying. This includes the positioning of computer screens in reception areas and other semi-public areas so that they are not easily viewed by visitors or children and young people to ensure that inappropriate disclosure of information does not take place.

16.4 Stealing software or using unlicensed software is illegal and can serve as grounds for prosecution and termination of employment

16.5 Aspris does not permit use or possession of copies of software without paying appropriate fees and signing of appropriate licenses. The IT Department is responsible for the procurement of all software and for conducting audits of software on Aspris computers to ensure that all software is properly licensed. All users, however, have a responsibility to ensure that all software they use is correctly licensed

16.6 Software licences are transferred between computers when they are replaced. Users must not continue to use computers that has been replaced and is therefore unlicensed. Such equipment must be returned to IT Department.

16.7 If a colleague inadvertently obtains information to which they are not entitled, or becomes aware of a breach of security pertaining to any service or central services team, the colleague must immediately report it to the person responsible or to the Aspris IT Helpdesk.

16.8 Colleagues must not attempt to probe computer security mechanisms. If colleagues probe security mechanisms, alarms will be triggered and Aspris IT Resources will needlessly be spent tracking the activity.

16.9 Unless prior written authority has been obtained from the IT Director, files found on a user's computer containing computer hacking tools or other suspicious material may be regarded as gross misconduct.

16.10 Data must not be removed from site unless it is a requirement of your job role or you have been provided with written authorisation by the service leader or central services team leader.

17 ACCESS TO EQUIPMENT

17.1 Only authorised colleagues whose work requires it will be allowed access to server computers.

17.2 The level of protection provided for server computers and communications equipment against fire, water, electric power fluctuations, physical damage, and theft is the responsibility of the IT Director. Advice on protection for remote systems is also available from the IT Department.

17.3 The IT Department is responsible for controlling day to day access to server computers and for providing adequate protection to computers, terminals, and communications equipment.

17.4 Aspris IT equipment issued to colleagues is specifically to be only used by colleagues only. Children and young people's use is restricted to IT equipment that is specifically designated for their use at a service.

17.5 Colleagues are responsible for ensuring that visitors to their service do not access Aspris equipment without authorisation by the IT Director and for ensuring that visitors do not connect, or attempt to connect, non-Aspris equipment.

17.6 IT equipment must not be removed from a service unless it is a requirement of your job role or you have been provided with written authorisation by the service leader or central services team leader.

18 IT SUPPORT

18.1 Colleagues are able to obtain support for their IT Equipment and system access by contacting the Aspris IT Helpdesk by telephone or email.

18.2 There may be exceptional circumstances where the Aspris IT Helpdesk may request a user to provide them with their user ID and password. The only circumstances where a request may be made include:

(a) Setting up or configuring replacement laptops
(b) Setting up or configuring a mobile telephone
(c) Replicating a fault or issue occurring on a user's Aspris IT Services accounts which cannot be recreated on another log-in.

18.3 In all cases the IT Department will never request a user to send their password to them by email, but instead request the user telephones the Aspris IT Helpdesk quoting an incident number.

18.4 Aspris IT Helpdesk will never in an outgoing call request made to the user ask them to provide their password over the phone, but will ask the user to call back quoting an incident number.

18.5 Telephoning the Aspris IT Helpdesk is to provide assurance to the user that they are speaking with a member of the team. The Aspris IT Helpdesk will then transfer them to the member of the team dealing with their request who will provide an explanation of the task to be completed and reason why the password is required.

18.6 Upon completion of the work, Aspris IT Helpdesk will inform the user that the task has been completed and the user should change any passwords that were disclosed as soon as possible.

19 CONTINGENCY PLANNING

19.1 The IT Department is responsible for developing and co-ordinating recovery plans in the event of the destruction of IT systems and also in the event of short-term loss of any of our data processing capability.

19.2 The IT Department is responsible for backing up systems and data, carrying out restores of data on demand, carrying out test restores of systems and data, monitoring backups of servers and developing good practice guidance for server backup.

19.3 These plans are based upon a systematic assessment of the risk of loss of the ability to process transactions for each application on each platform.

19.4 This does not reduce a colleagues responsibility to ensure the security and integrity of information stored on their computer.

19.5 Further information on the Aspris's Contingency and Business Continuity Planning can be obtained from the IT Director.

20 REPORTING SECURITY PROBLEMS

21.1 The Aspris IT Helpdesk must be notified immediately if:

(a) Confidential information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties
(b) The loss of Aspris issued IT equipment
(c) Unauthorised use of the Aspris IT Services has taken place, or is suspected of taking place
(d) Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed
(e) There is any unusual systems behaviour, such as missing files, frequent system crashes, misrouted messages
(f) Security problems should not be discussed widely but should instead be shared on a need-to-know basis.

21 PROCEDURES TO UPDATE THIS POLICY

21.1 This policy is designed to be a "live" document that will be altered by IT Department as required to deal with changes in technology, applications, procedures, legal and social imperatives, perceived dangers and any other condition which may affect security.

21.2 Aspris regards the integrity of its IT Services as central to the success of the business. As such, on behalf of Aspris, policy will be to take any measures considered necessary to ensure that all aspects of Aspris IT Services are fully protected. Aspris reserves the right to change or cancel the provisions of this policy, with or without notice, as the needs of the business dictate.

21.3 Updates to this policy will be issued to all colleagues covered within its scope.
Major changes will be approved by the IT Department. Minor changes will be approved by the IT Director.

SUPPLIMENTRY IT SERVICES

This section should be read and understood by users who have been provided the following additional IT services:

a) Mobile phone and Data Cards
b) Remote Access
c) Bluetooth Encryption
d) Mobile Computing Devices

22 MOBILE PHONES including Data Cards

22.1 This section details the requirements for mobile phones used within Aspris and applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties, who have use of a mobile phone issued by Aspris.

22.2 **Issuing Policy –** Mobile phones will be issued only to Aspris colleagues with duties that require them to be in immediate and frequent contact when they are away from their normal service. For the purpose of this policy, mobile phones are defined as smart and mobile telephones, a tablet or laptop with a data card. Effective distribution of mobile devices must be limited to colleagues for whom the productivity gained is appropriate in relation to the costs incurred.

22.2.1 **Smart phones** and data cards may be issued, for operational efficiency, to colleagues who need to conduct immediate, critical Aspris business. These individuals generally are at the executive and senior management level. In addition to verbal contact, it is necessary that they have the capability to review emails and respond to critical issues.

22.3 **Loss and Theft -** Files containing confidential or sensitive data may not be stored on mobile phones unless it is protected by approved encryption. Additional care and vigilance is required in the physical security of a mobile phone on public transport or transported by car. Lost or stolen equipment must immediately be reported to the Aspris IT Helpdesk. Charges for repair/replacement due to misuse of equipment or misuse of services may be the responsibility of the colleague, as determined on a case-by-case basis. The cost of any item beyond the standard authorised equipment is also the responsibility of the colleague.

22.4 **Personal Use –** Mobile phones are issued for Aspris business. Personal use should be limited to minimal and incidental use.

23 REMOTE ACCESS

23.1 The standards set out in this section are designed to minimise the potential exposure to Aspris from damages that may result from unauthorised use of Aspris resources. Damages include the loss of company confidential data, intellectual property, damage to public image, damage to critical Aspris systems, etc.

23.2 This section applies to all colleagues, contractors, temporary and other workers within Aspris, including all personnel affiliated with third parties with a Aspris computer used to connect to Aspris IT Services. It also applies to remote access connections used to do work on behalf of Aspris, including reading or sending email and viewing intranet web resources.

23.3 General:

(a) It is the responsibility of colleagues, contractors, vendors and agents with remote access privileges to Aspris IT Services to ensure that their remote access connection is given the same consideration as the user's on-site connection

(b) Please refer to the following sections of this policy for details of protecting information when accessing Aspris IT Services via remote access methods, and acceptable use of Aspris IT Services:

i. Acceptable Encryption (Section 14)
ii. Wireless Communications (Wi-Fi) (Section 10)
iii. Acceptable Use (Section 9)

23.4 **Requirements -** Remote access must be strictly controlled. Control will be enforced via password and two factor authentication

(a) For information on creating a strong passphrase see Section 6 User ID and Password Control

(b) At no time should any colleague provide their login or email password to anyone (with the exception of IT Department – See Section 18 IT Support), not even family members

(c) Colleagues and contractors with remote access privileges must ensure that their computer, which is remotely connected to Aspris IT Services, is not connected to any other network at the same time
(d) Colleagues and contractors must not use non-Aspris email accounts or other external resources to receive or send any communication or document in connection with Aspris business, thereby ensuring that official business is never confused with personal business. The only exception to this is with the express permission from the Chief Services Officer
(e) Colleagues and contractors must not use non-Aspris computers to undertake Aspris work activities
(f) Non-standard hardware configurations must be approved by IT Department
(g) All computers that are connected to Aspris IT Services must use the most up-to-date anti-virus software
(h) Only mobile computing or storage devices approved for use must be connected to Aspris IT Services
(i) The IT Department shall approve all new mobile computing and storage devices that may connect to Aspris IT Services. The IT Department will maintain a list of approved mobile computing and storage devices
(j) The Aspris IT Helpdesk must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

23.5 **Remote Access for 3rd Parties -** Suppliers of systems or software expect to have remote access to these systems in order to investigate and fix faults. Aspris will permit such access via a secure connection. 3rd Party User Accounts will need to be approved and authorised by the IT Director. Each supplier requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified colleagues. 3rd Party User Accounts will be disabled and will only be enabled for a time window when an approved change has been agreed.

24 BLUETOOTH ENCRYPTION

24.1 This section provides for more secure Bluetooth Device operations to protect the company from loss of confidential information. It applies to colleagues, contractors, consultants, temporary and other workers at the Aspris, including all personnel affiliated with third parties when using a Bluetooth Device.

24.2 **Version level -** No Bluetooth Device shall be deployed on Aspris equipment that does not meet Bluetooth v5.2 specifications without the written authorisation from IT Department. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy and meet Bluetooth version v5.0 specifications.

24.3 **Pins and Pairing -** When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area. If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, **you must refuse the pairing request and** report it to IT Department, via the Aspris IT Helpdesk, immediately. Unless your Bluetooth device itself has malfunctioned and lost its pin, this is a sign of a hack attempt.

24.4 **Device Security Settings -** All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment. If your device allows the usage of long PINs, you must use either a 13 alphabetic PIN or a 19 digit PIN (or longer). Always switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed. Ensure that you update the device's firmware when a new version is available.

24.5 **Unauthorised Use -** The following is a list of unauthorised uses of Aspris-owned Bluetooth devices:

(a) Eavesdropping, device ID spoofing, DoS attacks, or any for attacking other Bluetooth enabled devices
(b) Using Aspris owned Bluetooth equipment on non-Aspris owned Bluetooth enabled devices unless approved by the IT Director.
(c) Unauthorised modification of Bluetooth devices for any purpose.

24.6 **User Responsibilities**

(a) It is the Bluetooth user's responsibility to comply with this policy
(b) Bluetooth users must only access Aspris information systems using approved Bluetooth device hardware, software, solutions, and connections
(c) Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorised for use
(d) Bluetooth users must act appropriately to protect information, Aspris IT Services access, passwords, cryptographic keys, and Bluetooth equipment
(e) Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to the Aspris IT Helpdesk.

25 MOBILE COMPUTING DEVICES

25.1 The use of mobile devices can bring significant business benefits. However, their portability and desirability bring significant risk of loss and theft, which must be mitigated to ensure that company and service user data is protected.

25.1.1 To protect information assets stored on devices the following controls have been applied to mobile devices:

(a) Laptops and tablet harddrives issued to individual colleagues are encrypted
(b) External harddrives and USB data sticks used for storing non-public information assets are encrypted
(c) iPads and iPhones have password protection which encrypts the device when locked
(d) Smartphone have password protection
(e) iPads, iPhones and Smartphone devices have been enabled to allow the devices to be remotely wiped.

25.2 This section was created to mitigate the following identified risks associated with the use of mobile devices:

(a) A breach of confidentiality due to the access, transmission, storage, and disposal of sensitive information whilst using a mobile device
(b) A breach of integrity due to the access, transmission, storage, and disposal of sensitive information whilst using a mobile device
(c) A loss of availability to critical business systems as a result of using a mobile device.

25.3 This section applies to any mobile device, and its user, that has been issued by the Aspris that is used for business purposes and/or store Aspris information. Mobile devices currently approved for use by Aspris are Apple iPhone, Apple iPad and Samsung Galaxy Smartphone.

25.4 **Access -** A mobile device is to be used for business communications only. However we do recognise that there could be exceptional circumstances or prior agreement with your line manager, when you need to make use of a mobile device for your own personal use.

(a) Mobile device contract plans are set up for use within the UK only. Should you require use of your mobile device when on business outside the UK, then your line manager will need to contact the Aspris IT Helpdesk 7 days prior to your trip so that an appropriate international calling and data plan can be organised
(b) To protect Aspris IT Services from malware and viruses only approved applications must be installed and used on a mobile device. If you have a business need to install software including Apps to assist you in undertaking your duties then this must be approved by the IT Department before installation
(c) Users must read and abide by the AIT08 Mobile and remote working policy

(d) All mobile devices issued will be protected by a 6 digit alpha/numeric PIN/password entered by user upon accessing the device
(e) The PIN/password will not be subject to an enforced PIN/password change unless the user undertakes a voluntary change due to them believing that their details may have been compromised
(f) The use of strong PIN/password is recommended for all mobile devices to ensure that the device is adequately protected from unauthorised access. Users should refrain from using dates of birth and family member names which can easily be guessed. – see Section 6 User ID and Password Control
(g) Users should take care when entering their PIN/Password. If the PIN/password is incorrectly entered a total of 6 times consecutively will result in the device being automatically wiped of all its data
(h) Devices will be set with an auto-lock feature that will be activated after a period of inactivity.

25.5 **Encryption -** Encryption is used for the transmission of sensitive information to/from mobile devices. The locking of a mobile device will automatically cause the data stored on it to be encrypted.

25.6 **Security -** A lost or stolen mobile device must be reported to the Aspris IT Helpdesk immediately. If the incident occurs out of hours then Bamboo must be contacted on **0800 804 4040** to place a bar on the device.
(a) To protect the data on a mobile device, a feature is enabled that provides the Aspris IT Helpdesk with the capability to remotely wipe a device. A decision on whether to wipe a device will be taken after considering the circumstances of the loss and the type of data that may be held on the mobile device
(b) Users must physically secure their mobile device when left unattended by ensuring that it is locked
(c) Users who have been issued with an iPad will have been provided with a case in which to store the device. Wherever possible, especially when being used in a public place, the case must be used to ensure that the Aspris asset tag is not visible to avoid the unwelcome attention from third parties
(d) When using a mobile device within a public place, the user must be on their guard against confidential conversations being over heard, confidential data being read by shoulder surfers and the potential theft of the device
(e) Users must not allow another colleague or third party to access or use their mobile device
(f) Users must return their mobile device to their line manager at the end of their employment. At which time, the line manager must return it to IT Department for the device to be wiped and reissued.

25.7 **Vulnerability Management -** Critical security updates/patches for in-use software will be deployed when required to all mobile devices and when prompted the user must install them immediately.

25.8 **Definitions**
User – Any colleagues issued with a mobile device
Mobile device - A portable electronic device: iPhone, iPad, Smartphone, Tablet
PIN - Personal Identification Number
Remote Wipe - Use of software to destroy data on mobile device

26 REFERENCES

Data Protection Act 2018
Computer Missue Act 1990
HIPAA Security Rule - Standard 164.310(c) Workstation Security