PRIORY GROUP OF COMPANIES

| | |
|---|---|
| **POLICY TITLE:** | **IT Security** |
| **Policy Number:** | IT02 |
| **Version Number:** | 10 |
| **Date of Issue:** | 21/09/2017 |
| **Date of Review:** | 20/09/2020 |
| **Author:** | IT Department |
| **Ratified by:** | Brian McCallion, IT Risk & Compliance Manager |
| **Responsible signatory:** | Clair Dunn, Group IT Director |
| **Outcome:** | This Policy:<br>• details colleagues' responsibilities for computer security within the Priory Group, and is designed to help them understand their position |
| **Cross Reference:** | OP02 Data Protection<br>OP27 Confidentiality<br>H&S60 Driving at Work<br>HR04.8 Protection of Colleague Data<br>HR04.10 Anti-Bullying and Harassment<br>HR06 Termination of Employment (Leavers)<br>HR11 Use of Social Media by Colleagues<br>IT10 Information Asset Management<br>IT11 Information Transfers |

**EQUALITY AND DIVERSITY STATEMENT**

Priory Group 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

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, e-mail RARHelpdesk@priorygroup.com

# IT SECURITY

**Contents** **Page**

# 1 VERSION CONTROL

1.1

| Issue No. | Comments | Updated | Date |
|---|---|---|---|
| Draft 0 | Initial release for comment | | |
| **Live (V1.0)** | Reviewers comments incorporated | | |
| V1.01 | Changes to personnel and job titles | | |
| V1.02 | Changes made to make Policy Group-wide and to emphasise monitoring of Web & Email. | | |
| V1.1 | Policy revised and separated into Westminster and Priory versions. Amendments also made to take account of Priory HQS project. | | |
| V1.2 | Amendments made to strengthen policy and to take account of new technologies. | | |
| V1.2 | Small amendments regarding CEO/CFO change of personnel in Introduction. Remainder of policy remains same. | | |
| V03 | Complete review and introduction of new policies. | Group IT Department | 08/07/2009 |
| V04 | Policy revised following review of Affinity Healthcare policies. Amendments made to email and internet usage. New section added to remote access on 3rd Parties. | Group IT Department | 01/07/2010 |
| V05 | Minor revision to Section 18 Internet Access concerning website filtering and the unblocking of sites 18.3.3 (a) | Group IT Department | 19/09/2011 |
| V06 | Addition of mobile device policy & removal of appendix 1- IT Security policy changes for users of the Affinity network. | Group IT Department | 03/01/2014 |
| V07 | Renumbered paragraphs. Addition of advice regarding use of personal email accounts 15.4 (d) (e) | Group IT Department | 17/11/2015 |
| V08 | Includes changes required for ISO 27001. | Group IT Department | 05/01/2016 |
| V09 | Change to clarify sharing of sensitive data by email under 5.3.1. Terminology changed throughout to colleague instead of employee. | Group Policy, IG and Accreditation Manager | 24/01/2017 |

## 2 INTRODUCTION

2.1 Priory Group depends on its computers, data, information processing capabilities and telecommunications systems for our day to day business. IT systems are now a critical part of our information infrastructure.
It is vitally important, therefore, that the security of these systems and the data held by Priory Group 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 position.
Compliance with this policy is part of your contract of employment with Priory Group. 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 the policy in full.
If there are any queries with regard to this document, please feel free to contact a member of the IT Security Group, listed below, for clarification.
Thank you for your cooperation.
Tina Walton, Chief Information Officer and Transformation Director
Clair Dunn, Group IT Director

Dated: April 2017

## 3 SCOPE

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

3.2 It applies to:
(a) Our servers, personal computers, personal communications devices, remote access facilities, outside suppliers of data, LANs (Local Area Networks), WANS (Wide Area Networks), and telephone systems
(b) All software used on Priory Group computer systems, whether packaged or bespoke and third party software provided as a service accessed through a public network
(c) All Priory Group data and reports derived from Priory Group data
(d) All programs developed in Priory Group time, using Priory Group equipment, or by Priory Group colleagues
(e) All computers, communications links, and associated equipment on Priory Group premises or connected to Priory Group computers.

3.3 Note that the use of Priory Group IT equipment by service users or customers is restricted to specifically designated equipment at certain sites connected to the Service User Network. Non-colleagues are not permitted to use any other Priory Group IT equipment.

## 4 RESPONSIBILITIES

4.1 **The Priory Group Chief Information Officer** has overall responsibility for ensuring that Priory Group has adequate computer security measures in place.

4.1.1 IT security risks must be identified and addressed in every project and dealt with in accordance with the IT Departments HC17 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 the Priory Group Chief Information Officer immediately whenever he or she sees actions that go against, or seem to go against, this policy.

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

4.2.2 IT equipment or 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 site authority.

4.2.3 If you have access to personal data such as salaries, home telephone numbers, patient, student or resident information etc., you must at all times, adhere to the provisions of the Data Protection Act 1998. In particular, you must ensure they comply with the Act when transferring or disclosing any data or information to external organisations. (See HR04.8 Protection of Colleague Data, OP02 Data Protection and OP27 Confidentiality).

4.2.4 You must use Priory Group IT facilities only for authorised purposes. To use IT facilities for other purposes may be an offence under the Computer Misuse Act 1990. In particular no staff are authorised to install software on any Priory computer systems.

4.2.5 It is your responsibility to ensure that all machines used during the day are logged out and closed down in a controlled manner, before leaving the office. Unattended machines that are left logged on constitute a serious security risk, and can be interpreted as a misuse of the Priory Group IT facilities.

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

4.2.7 You are responsible for the security and integrity of information stored on your personal desktop system. This responsibility includes making regular backups of any data held on local desktop 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 them unattended and secure at any time. 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 USERID, passwords or PINs issued to you for the purposes of accessing Priory Group IT and telecommunications systems including PCs 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 Priory IT – See Section 23 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 must ensure:

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

(b) **Priory Group IT Department are informed** of every colleague who has access to IT services, when they **transfer sites/teams/departments/division, change roles or they no longer work for the Priory**, 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 platforms. You are responsible for notifying Priory Group IT Department when a

USERID should be revoked or deleted. Refer to HR4.06 Termination of Employment (Leavers)

(d) You are responsible for the safe return to Priory Group 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 HR4.06 Termination of Employment (Leavers).

**All colleagues must 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 When an email is sent originating from Priory Group, 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 the Priory Group, to prevent tarnishing the public image of Priory Group.

5.2 This section covers appropriate use of any email sent from a Priory Group email address and applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties.

5.3 **Prohibited Use:**

(a) The Priory Group 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 Priory Group colleague should report the matter to their supervisor 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 a Priory Group 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 by a Priory Group colleague

(f) Virus or other malware warnings and mass mailings from the Priory shall be approved by the Priory Group IT Department before sending.

5.3.1 **Sensitive Personal Information -** Email is not a secure system. Therefore sensitive personal information or company confidential information should not be sent by email to an external address unless it has been encrypted. Because of the extra security precautions in place within the Priory system, emails sent to internal email accounts within the Priory system can contain personal sensitive information or company confidential information, but the sender has the responsibility to check that the recipient has a legitimate requirement to see the sensitive information. **NB:** Information received internally containing sensitive personal 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 personal sensitive information is contained within the trail or the attachments.

5.3.2 **Personal Use -** Using a reasonable amount of Priory Group 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 Priory Group systems

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 Priory Group information systems and in support of Priory Group business.

## 6 USERID AND PASSWORD CONTROL

6.1 **Overview -** UserID's (user identification) and 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 the Priory Group's entire corporate network. As such, all Priory Group colleagues (including contractors and vendors with access to Priory Group 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, consultants, temporary and other workers within Priory Group, 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 Priory Group site, has access to the Priory Group network, or stores any non-public Priory Group information.

6.3 **General**

(a) No one is to be permitted to use Priory Group computers without an authorised USERID
(b) To obtain a USERID requires the approval of your Line Manager
(c) Each user is responsible for all activity that occurs on any system that is accessed by use of his or her USERID
(d) USERID's may be revoked (or cancelled or suspended) at any time through the agreement of the Priory Group Chief Information Officer
(e) USERID's will be revoked when a colleague terminates or transfers
(f) All system-level passwords (e.g., root, server admin, application administration accounts, etc.) must be changed every 90 days
(g) All user-level passwords (e.g., email, web, desktop computer, etc.) are set by Priory Group Policy to be changed every 90 days
(h) Passwords must be memorised and never written down or inserted into email messages or other forms of electronic communication
(i) Passwords should never be shared with anyone else (with the exception of Priory IT – See Section 23 IT Support).
(j) User accounts that have system-level privileges granted through Group memberships or programs must have a unique password from all other accounts held by that user
(k) Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public", "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMPv2)
(l) 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 Priory Group. Some of the more common uses include: user level accounts, web accounts, email accounts, voicemail password, and local router logins. Everyone should be aware of how to select strong passwords.

6.4.1 Poor, weak passwords have the following characteristics:

(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

"Priory", 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 Strong passwords have the following characteristics:

(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 fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e)

(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: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

6.5 **Password Protection Standards -** Do not use the same password for Priory Group accounts as for other non-Priory Group access (e.g. personal email account, online banking, etc.). Where possible, don't use the same password for various Priory Group access needs. For example, select one password for the general admin network and a separate password for programs such as CareNotes, Coldharbour etc. Do not share Priory Group passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Priory Group information. Here is a list of 'dont's':

(a) Don't reveal a password over the phone to ANYONE (with the exception of Priory IT – See Section 23 IT Support)

(b) Don't reveal a password in an email message

(c) Don't reveal a password to your boss

(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 of applications (e.g. Outlook, MSN Messenger)

(j) Don't write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Blackberry's or similar devices) without encryption.

6.5.1 If someone demands a password (with the exception of Priory IT – See Section 23 Support), refer them to this document or have them call someone in the Priory Group IT Department, and if an account or password is suspected to have been compromised, report the incident to the Priory Group IT Department and change all passwords.

6.6 **Application Development Standards -** Application developers must ensure their programs contain the following security precautions. Applications:

(a) Should support authentication of individual users, not Groups

(b) Should not store passwords in clear text or in any easily reversible form

(c) Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

6.7 **Use of Passwords and Passphrases for Remote Access Users -** Access to the Priory Group Networks via remote access is to be controlled using either a one-time password

authentication or a public/private key system with a strong passphrase.

6.8 **Passphrases -** Passphrases are not the same as passwords, they are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. A passphrase is a longer version of a password and is, therefore, more secure. It is typically composed of multiple words, and because of this, is more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
All of the rules above that apply to passwords apply to passphrases.

## 7 WORKSTATION SECURITY (CLEAR DESK AND CLEAR SCREEN)

7.1 The purpose of this section is to provide guidance for workstation security for Priory Group workstations in order to ensure the security of information on the workstation and information the workstation may have access to. It applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties with a Priory Group workstation connected to the Priory Group network.

7.2 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorised users.

7.3 Colleagues using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimise the possibility of unauthorised access.

7.4 Priory will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorised users.

7.5 Appropriate measures include:

(a) Restricting physical access to workstations to only authorised personnel
(b) Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access
(c) Complying with all applicable password policies and procedures
(d) Ensuring workstations are used for authorised business purposes only
(e) Never installing unauthorised software on workstations
(f) Storing all confidential information, including protected health information (PHI) on network servers
(g) Keeping food and drink away from workstations 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 9 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
(k) Ensuring that all workstations 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 13 Wireless Communications)
(m) Any information assets including paper documents are removed from desks and locked away at the end of the working day.

## 8 PERSONAL COMMUNICATION DEVICES

8.1 This section details the requirements for Personal Communication Devices used within Priory Group and applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties, who have use of Personal Communication Devices issued by Priory Group for Priory Group business.

8.2 **Issuing Policy -** Personal Communication Devices (PCDs) will be issued only to Priory Group personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include any wireless device, mobile telephones, tablet or laptop with data cards, Blackberrys and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

8.2.1 **Blackberrys** and data cards may be issued, for operational efficiency, to Priory Group personnel who need to conduct immediate, critical Priory Group 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 and have documented responses to critical issues. The Priory Group IT Department shall conduct a risk analysis to document safeguards for each media type to be used on the network.

8.2.2 **Bluetooth**, or similar hands-free enabling devices, may be issued to authorised Priory personnel who have received approval.

8.3 **Loss and Theft -** Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Additional care and vigilance is required in the physical security of a PCD. This is particularly important when a PCD is being used in a public place, being carried on public transport or transported by car. Lost or stolen equipment must immediately be reported. 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.

8.4 **Personal Use -** PCDs and voicemail are issued for Priory Group business. Personal use should be limited to minimal and incidental use.

8.5 **PCD Safety -** Conducting telephone calls or utilising PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If colleagues must use a PCD while driving, Priory Group requires the use of hands-free enabling devices.

## 9 VIRUS PROTECTION

9.1 Priory Group must ensure that it protects its computer systems from external attacks. Priory Group 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.

9.2 This section outlines the processes that colleagues can take to prevent virus problems and is applicable to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties who have access to the Priory Group Network.

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

(a) Not use any electronic media including, but not limited to; floppy disks, CDs, memory sticks or cards that have been used outside Priory Group; in any Priory Group equipment that is connected, or may be connected, to the Priory Group network, without the prior approval of the Priory Group Business Systems Director
(b) Not use any electronic media that have been used in Priory Group equipment designated for the use of residents, patients or pupils in any Priory Group equipment that is connected, or may be connected, to the Priory Group network, without the prior approval of the Priory Group Business Systems Director
(c) Not allow the connection of any non-Priory Group equipment (e.g. that owned by consultants, suppliers, residents, patients or pupils) to the Priory Group network without the prior approval of the Priory Group Business Systems Director. If such permission is granted, the equipment must be checked for viruses by a member of the Priory Group IT Department before connection takes place
(d) Contact the Priory Group IT Department 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 Priory Group IT Department
(e) Users should be aware that many hoax virus warnings exist. If any warning is received it should be sent to the Priory Group IT Help Desk where its authenticity will be checked. Such warnings must not be forwarded to other colleagues
(f) 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
(g) Delete spam, chain, and other junk email without forwarding, in line with Section 11 Acceptable Use
(h) Never download files from unknown or suspicious sources
(i) Back-up critical data and system configurations on a regular basis and store the data in a safe place.

## 10 SOFTWARE INSTALLATION

10.1 Allowing colleagues to install software on company computing 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 network are examples of the problems that can be introduced when colleagues install software on company equipment.

10.2 The purpose of this section is to minimise the risk of loss of program functionality, the exposure of sensitive information contained within the Priory Group's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software and it applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties who use desktops, laptops, servers, Blackberrys, smartphones and other computing devices operating within Priory Group.

10.3 Colleagues may not install software on Priory Group computing devices operated within the Priory Group network. Software requests must first be approved by the requester's manager and then be made to the Priory Group IT Department in writing or via email. Software must be selected from an approved software list, maintained by the Priory Group IT Department, unless no selection on the list meets the requester's need. The Priory Group IT Department will obtain and track the licenses, check new software for conflict and compatibility, and perform the installation unless specific written permission is provided by the Priory Group IT Department.

10.4 To minimise security risks, software which is freeware or open source will not be considered where software which meets the needs of the business is available from a trusted software house.

## 11 ACCEPTABLE USE

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

11.1.1 Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet access and FTP, are the property of Priory Group. These systems are to be used for business purposes in serving the interests of the company, and of our service users and customers in the course of normal operations.

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

11.2 The purpose of this section is to outline the acceptable use of IT equipment throughout Priory Group. These rules are in place to protect the colleague and the Priory. Inappropriate use exposes Priory Group to risks including virus attacks, compromise of network systems and services, and legal issues.

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

11.4 **General Use and Ownership**

(a) While Priory Group's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Priory Group. Because of the need to protect the Priory Group's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Priory Group

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

(c) Priory Group IT Department recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Section 20 Information Classification

(d) For security and network maintenance purposes, authorised individuals within Priory Group may monitor equipment, systems and network traffic at any time

(e) Priory Group reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

11.4.1 **Security and Proprietary Information**

(a) The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Information Classification section of this document (See Section 20 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. System level passwords should be changed quarterly; user level passwords should be changed every 90 days

(c) All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the PC is to be left unattended
(d) Because information contained on portable communication devices 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 a Priory Group email address to newsGroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Priory Group, unless posting is in the course of business duties
(f) All hosts used by the colleague that are connected to the Priory Group Internet/Intranet/Extranet, whether owned by the colleague or the Priory, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or Group policy
(g) Colleagues must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code
(h) Colleagues should be on their guard against phishing attacks. Phishing is the act of sending an e-mail to a user falsely claiming to be from a trustworthy source in an attempt to trick the user into surrendering private 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.

11.4.2 **Unacceptable Use** - The following activities are, in general, prohibited. Colleagues may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a colleague of Priory Group authorised to engage in any activity that is illegal under English or international law while utilising Priory Group-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.

11.4.2.1 **System and Network 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 Priory Group
(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 Priory Group or the end user does not have an active license, is strictly prohibited
(c) Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.)
(d) Revealing your account password to others (with the exception of Priory IT – See Section 23 IT Support). or allowing use of your account by others. This includes family and other household members when work is being done at home
(e) Using a Priory Group computing asset to actively engage in procuring or transmitting material that is in violation of HR04.10 Anti-Bullying and Harassment
(f) Making fraudulent offers of products or services originating from any Priory Group 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 network communication. 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, network 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 Priory Group IT Department is made
(j) Executing any form of network monitoring which will intercept data not intended for the colleague's host, unless this activity is a part of the colleague's normal job/duty
(k) Circumventing user authentication or security of any host, network or account
(l) Interfering with or denying service to any user other than the colleague's host (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, Priory Group patients, residents, students or colleagues to parties outside Priory Group
(o) Priory Group colleagues and contractors must not use non-Priory Group PC's to undertake Priory Group work activities
(p) Transferring company information to/from a personal computing device via email or storage device to facilitate Priory work activities.

11.4.2.2 **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 the Priory Group's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Priory Group or connected via Priory Group's network
(g) Posting the same or similar non-business-related messages to large numbers of Usenet newsGroups (newsGroup spam)
(h) Priory Group colleagues and contractors must not use non-Priory Group email accounts or other external resources to receive or send any communication or document in connection with Priory Group business, thereby ensuring that official business is never confused with personal business. The only exception to this is with the express permission from the Priory Group Chief Information Officer.

11.4.2.3 **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 Priory confidential or proprietary information, trade secrets or any other material that would be covered by OP02 Data Protection
(b) Colleagues shall not engage in any posting that may harm or tarnish the image, reputation and/or goodwill of the Priory 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 HR4.10 Anti Bullying and Harassment
(c) Colleagues may also not attribute personal statements, opinions or beliefs to the Priory Group 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 Priory Group 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, Priory's trademarks, logos and any other Priory Group 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 HR11 Use of Social Media by Colleagues.

## 12 VIRTUAL PRIVATE NETWORKS (VPN)

12.1 The purpose of this section is to provide guidelines for Remote Access IPSec Virtual Private Network (VPN) connections to the Priory Group corporate network. It applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties utilising VPNs to access the Priory Group network. This section applies to implementations of VPN that are directed through an IPSec Concentrator.

12.2 Approved Priory Group colleagues and authorised third parties (customers, vendors, etc.) may utilise the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in Section 15 Remote Access.

12.2.1 Additionally:

(a) It is the responsibility of colleagues with VPN privileges to ensure that unauthorised users are not allowed access to Priory Group internal networks

(b) VPN use is to be controlled using a public/private key system with a strong passphrase

(c) When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped

(d) Dual (split) tunnelling is NOT permitted; only one network connection is allowed

(e) VPN gateways will be set up and managed by the Priory Group IT Department

(f) All computers connected to the Priory Group internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard

(g) VPN users will be automatically disconnected from the Priory Group's network after fifteen minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open

(h) The VPN tunnel is limited to an absolute connection time of 24 hours

(i) Only the VPN client supplied by the Priory Group IT Department may be used.

## 13 WIRELESS COMMUNICATIONS

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

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

13.1.2 This is also applicable to all wireless infrastructure devices that connect to the Priory Group

network or reside on a Priory site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, mobile phones and Blackberrys. This includes any form of wireless communication device capable of transmitting packet data. **The Priory Group IT Department must approve exceptions to this in advance.**

13.2 **General Network Access Requirements** - All wireless infrastructure devices that reside at a Priory site and connect to the Priory Group network, or provide access to information classified as Priory Confidential, Priory Highly Confidential, or Priory Restricted must:

(a) Abide by the standards specified in the Wireless Communication Standard
(b) Be installed, supported, and maintained by Priory Group IT Department
(c) Use the Priory Group approved authentication protocols and infrastructure
(d) Use the Priory Group 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.

13.3 **Home Wireless Device Requirements** - Wireless infrastructure devices that provide direct access to the Priory Group corporate network, must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.

13.3.1 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Priory Group corporate network. Access to the Priory Group corporate network through this device must use standard remote access authentication.

## 14 REMOVABLE MEDIA

14.1 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 the Priory and to reduce the risk of acquiring malware infections on computers operated by Priory Group.

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

14.3 Priory Group colleagues may only use Priory Group supplied removable media in their work computers. Priory Group removable media may not be connected to or used in computers that are not owned or leased by Priory Group without explicit permission of the Priory Group IT Department. Sensitive information should be stored on removable media only when required in the performance of your assigned duties. When sensitive information is stored on removable media, it must be encrypted in accordance with the Acceptable Encryption section (see Section 17 Acceptable Encryption). **Please note the use of USB sticks within Priory Group is strictly prohibited unless given specific written permission by the Priory Group IT Department.**

## 15 REMOTE ACCESS

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

15.2 This section applies to all colleagues, contractors, consultants, temporary and other workers within Priory Group, including all personnel affiliated with third parties with a Priory Group owned computer or workstation used to connect to the Priory Group network. It also to remote access connections used to do work on behalf of Priory Group, including reading or sending email and viewing intranet web resources. Remote access implementations that

are covered by this policy include, but are not limited to, dial-in modems, ISDN, ADSL, VPN, SSL, and cable modems, etc.

15.3 General:

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

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

i. Acceptable Encryption (Section 17)
ii. Virtual Private Network (VPN) (Section 12)
iii. Wireless Communications (Section 13)
iv. Acceptable Use (Section 11).

15.4 **Requirements -** Secure remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong passphrases

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

(b) At no time should any Priory Group colleague provide their login or email password to anyone (with the exception of Priory IT – See Section 23 IT Support), not even family members

(c) Priory Group colleagues and contractors with remote access privileges must ensure that their Priory owned computer or workstation, which is remotely connected to the Priory's corporate network, is not connected to any other network at the same time

(d) Priory Group colleagues and contractors must not use non-Priory Group email accounts or other external resources to receive or send any communication or document in connection with Priory Group business, thereby ensuring that official business is never confused with personal business. The only exception to this is with the express permission from the Priory Group Chief Information Officer

(e) Priory Group colleagues and contractors must not use non-Priory Group PC's to undertake Priory Group work activities

(f) Non-standard hardware configurations must be approved by Priory Group IT Department

(g) All hosts that are connected to Priory Group internal networks via remote access technologies must use the most up-to-date anti-virus software

(h) Only mobile computing or storage devices approved for use must be connected to the Priory Group network

(i) The Priory Group IT Department shall approve all new mobile computing and storage devices that may connect to information systems at Priory. The Priory Group IT Department will maintain a list of approved mobile computing and storage devices

(j) The Priory IT Helpdesk must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

15.5 **Remote Access for 3rd Parties -** Suppliers of central systems or software expect to have remote access to these systems in order to investigate and fix faults. Priory Group will permit such access via a secure VPN connection. 3rd Party User Accounts will need to be approved and authorised by the Group IT Manager. Each supplier requiring remote access will be required to commit to maintaining confidentiality of data and information and only using qualified colleagues.

## 16 INTERNET ACCESS

16.1 The standards set out in this section are designed to minimise the potential risk to the Priory Group from damages which may result from unauthorised use of copyrighted material or damage to critical Priory Group internal systems, due to malware infections.

16.2 This section applies to all colleagues, contractors, consultants, temporary and other workers at the Priory Group, including all personnel affiliated with third parties issued with a UserID using a Priory Group owned computer or workstation used to connect to the Priory Group network who have been provided with access to the Internet.

16.3 **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 Priory Group work only. Colleagues may access websites and webmail accounts for personal use so long as it does not interfere with their work or the availability and speed of the Priory Network. Personal use of the Internet must comply with this policy.

16.4 **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 Priory Group Business Systems Director. In particular, the downloading of music, video or other media that is subject to copyright.

16.5 **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. Staff can make a request for a specific site to be blocked or unblocked (where a business or educational need exists) by contacting the Priory Group IT Department
(b) The Priory Group IT Department monitors Internet access for inappropriate use and will report any instances to senior management for appropriate disciplinary action.

16.6 **Network Administrator Use -** In order to maintain the Priory Group Network, it is necessary to download software updates from the Internet and apply these to Priory Group computer systems. Priory Group IT staff supporting the Priory Group computer systems will be permitted to download such updates.

## 17 ACCEPTABLE ENCRYPTION

17.1 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 United Kingdom. This section applies to all colleagues, contractors, consultants, temporary and other workers at the Priory, including all personnel affiliated with third parties.

17.2 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. Priory's key length requirements will be reviewed annually and upgraded as technology allows.

17.2.1 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 Priory Group 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

17.3 To protect information assets the following controls have been selected:
(a) Laptops and tablet harddrives issued to individual staff 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) iPads, iPhones and Blackberry devices have been enabled to allow the devices to be remotely wiped
(e) Remote access to the is secured using VPN technology
(f) Websites and SaaS are protected using secure sessions under https.

## 18 BLUETOOTH ENCRYPTION

18.1 This section provides for more secure Bluetooth Device operations to protect the company from loss of Personally Identifiable Information (PII) and proprietary company data. It applies to colleagues, contractors, consultants, temporary and other workers at the Priory, including all personnel affiliated with third parties when using a Priory Group Bluetooth Device.

18.2 **Version level -** No Bluetooth Device shall be deployed on Priory Group equipment that does not meet Bluetooth v2.1 specifications without the written authorisation from Priory Group IT Department. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except meeting the Bluetooth version v2.1 specifications.

18.3 **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 Priory Group IT Department, via the Priory IT Helpdesk, immediately. Unless your Bluetooth device itself has malfunctioned and lost its pin, this is a sign of a hack attempt.

18.4 **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.

18.5 **Unauthorised Use -** The following is a list of unauthorised uses of Priory-owned Bluetooth devices:
(a) Eavesdropping, device ID spoofing, DoS attacks, or any for attacking other Bluetooth enabled devices
(b) Using Priory-owned Bluetooth equipment on non-Priory-owned Bluetooth enabled devices unless approved by the Group Business Systems Director
(c) Unauthorised modification of Bluetooth devices for any purpose.

18.6 **User Responsibilities**

(a) It is the Bluetooth user's responsibility to comply with this policy
(b) Bluetooth users must only access Priory Group 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, network 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 Priory Group IT Helpdesk.

## 19 MOBILE DEVICES

19.1 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.

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

(a) Laptops and tablet harddrives issued to individual staff 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) iPads, iPhones and Blackberry devices have been enabled to allow the devices to be remotely wiped.

19.2 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.

19.3 This section applies to any mobile device, and its user, that has been issued by the Priory Group that is used for business purposes and/or store Priory Group information. It excludes the use of 'bring your own devices' (BYOD) which is currently prohibited from use as it creates additional challenges in the segregation and protection of personal and business data on a user's device. Mobile devices currently approved for use by the Priory Group are BlackBerry phones and Playbook, Apple iPhone and iPad.

19.4 **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 Priory IT Helpdesk 7 days prior to your trip so that an appropriate international calling and data plan can be organised
(b) To protect the Priory network 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 Priory IT Department before installation
(c) Users must read and abide by the IT08 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, then an iPhone or iPad will become automatically blocked from any future use and a Blackberry 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. BlackBerrys will auto-lock after 15 minutes. iPhones and iPads will auto-lock after 5 minutes.

19.5 **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.

19.6 **Security -** A lost or stolen mobile device must be reported to the Priory IT Helpdesk immediately. If the incident occurs out of hours then Total must be contacted on 0844 257 8818 to place a bar on the device.
(a) To protect the data on a mobile device, a feature is enabled that provides the Priory 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 Priory 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 Priory 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 Priory IT Department for the device to be wiped and reissued.

19.7 **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.

19.8 **Definitions**
**User** – Any Priory colleagues issued with a mobile device
**Mobile device** - A portable electronic device: BlackBerry, Playbook, iPhone, iPad
**PIN** - Personal Identification Number
**Remote Wipe** - Use of software to destroy data on mobile device
**BYOD** – A mobile device owned by a colleague used for business and personal purposes.

## 20 INFORMATION CLASSIFICATION

20.1 This section is intended to help colleagues determine what information can be disclosed to non-colleagues, as well as the relative sensitivity of information that should not be disclosed outside of Priory Group without proper authorisation.

20.1.1 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).

20.1.2 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 Priory Group information (e.g. Priory Group confidential information should not be left unattended in conference rooms).

20.1.3 Questions about the classification of a specific piece of information should be addressed to your Line Manager.

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

20.3 IT10 Information Asset Management provides details of the classifications, how to protect information and who can be party to the information within the Priory Group.

20.4 IT11 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.

## 21 ACCESS TO DATA

21.1 Levels of access to data will be determined by the Heads of Departments, Facility Directors/Managers, or equivalent, in conjunction with the Priory Group Chief Information Officer, who will ensure that levels of access are consistent throughout Priory Group.

21.2 No external software may be used. This includes the use of freeware and shareware packages, software downloaded from the Internet, software contained in email messages and software obtained from magazine cover disks or CDs.

21.3 All users with network access should ensure that all data is held on network drives, which are backed up, nightly by the Priory Group IT Department.

21.4 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, nursing stations and other semi-public areas so that they are not easily viewed by visitors, residents or patients to ensure that inappropriate disclosure of information does not take place.

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

21.6 Priory Group does not permit use or possession of copies of software without paying appropriate fees and signing of appropriate licenses. The Priory Group IT Department is responsible for the procurement of all software and for conducting audits of software on Priory-owned personal 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

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

21.8 If a user inadvertently obtains information to which he or she is not entitled, or becomes aware of a breach of security pertaining to any service, the user must immediately report it to the person responsible for that service or to the Priory IT Helpdesk.

21.9 Users must not attempt to probe computer security mechanisms. If users probe security mechanisms, alarms will be triggered and Priory Group IT Resources will needlessly be spent tracking the activity.

21.10 Unless prior written authority has been obtained from the Priory Group Chief Information Officer, files found on a user's computer containing computer hacking tools or other suspicious material may be regarded as gross misconduct.

21.11 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 site authority or Priory Group Chief Information Officer.

## 22 ACCESS TO EQUIPMENT

22.1 Only authorised persons whose work requires it will be allowed access to server computers.

22.2 The level of protection provided for central server computers and communications equipment against fire, water, electric power fluctuations, physical damage, and theft is the responsibility of the Priory Group Chief Information Officer. Advice on protection for remote systems is also available from the Priory Group IT Department.

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

22.4 In general Priory Group IT equipment is provided for use by colleagues only. Specifically, use by service users etc. is restricted to equipment that is specifically designated for that purpose at a limited number of sites. At such sites, equipment designated for non-colleague use must be kept separate from, and not connected to, the Priory Admin network.

22.5 Colleagues are responsible for ensuring that visitors to their sites do not access Priory equipment without authorisation by the Priory Group Chief Information Officer and for ensuring that visitors do not connect, or attempt to connect, non-Priory equipment to the Priory network

22.6 IT equipment 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 site authority.

## 23 IT SUPPORT

23.1 Users are able to obtain support for their Priory IT Equipment and system access by contacting the Priory IT Helpdesk by telephone or email.

23.2 There may be exceptional circumstances where Priory IT 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 AD or application account which cannot be recreated on another log-in.

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

23.4 Priory IT 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 the Priory IT Helpdesk quoting an incident number.

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

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

## 24 CONTINGENCY PLANNING

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

24.2 The Priory Group IT Department is responsible for backing up central systems and data, carrying out restores of central data on demand, carrying out test restores of central systems and data, monitoring backups of remote servers and developing good practice guidance for remote server backup. Remote server backup itself, however, is the responsibility of the local Facility Director/Manager.

24.3 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.

24.4 This does not reduce the user's responsibility to ensure the security and integrity of information stored on their personal desktop systems.

24.5 Further information on the Priory's Contingency and Business Continuity Planning can be obtained from the Priory Group Chief Information Officer.

## 25 REPORTING SECURITY PROBLEMS

25.1 The Priory Group IT Helpdesk must be notified immediately if:

(a) Sensitive Priory Group information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties
(b) The loss of Priory Group issued IT equipment
(c) Unauthorised use of Priory Group information systems 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.

## 26 PROCEDURES TO UPDATE THIS POLICY

26.1 This policy is designed to be a "live" document that will be altered by Priory Group 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 Priory's business security.

26.2 Priory Group regards the integrity of its computer system/network as central to the success

of the business. As such, on behalf of the Priory Group, policy will be to take any measures considered necessary to ensure that all aspects of the system/network are fully protected. Priory Group reserves the right to change or cancel the provisions of this policy, with or without notice, as the needs of the Group dictate.

26.3 Updates to this policy will be issued to all colleagues covered within its scope.

26.4 Major changes will be approved by the Priory Group IT Department. Minor changes will be approved by the Priory Group Chief Information Officer.

## 27 GLOSSARY

| Term | Definition |
|---|---|
| **ADSL** | Asynchronous Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet). |
| **Application Administration Account** | Any account that is for the administration of an application. |
| **Appropriate Measures** | To minimise risk to Priory from an outside business connection. Priory computer use by competitors and unauthorised personnel must be restricted so that, in the event of an attempt to access Priory corporate information, the amount of information at risk is minimised. |
| **Approved Electronic Mail** | Includes all mail systems supported by the Group IT Department. This includes, but is not necessarily limited to Microsoft Outlook. If you have a business need to use other mailers contact the Group IT Helpdesk. |
| **Approved Electronic File Transmission Methods** | Includes supported FTP clients and Web browsers. |
| **Approved Encrypted email and files** | Techniques include the use of DES. DES encryption is available via many different public domain packages on all platforms. |
| **Asymmetric Cryptosystem** | A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data e.g. public-key encryption. |
| **Blogging** | A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption. |
| **Bluetooth** | Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), and mobile phones via a secure, globally unlicensed short-range radio frequency. |
| **Cable Modem** | Cable companies such as Virgin Media provide Internet access over Cable TV coaxial cable. |
| **Chain Email or Letter** | Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed. |
| **Company Information System Resources** | Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above. |
| **Confidential or** | All data that is not approved for public release shall be |

| | |
|---|---|
| **sensitive data** | considered confidential or sensitive |
| **Configuration of Priory-to-other business connections** | Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary. |
| **Corporate connectivity** | A connection that provides access to the Priory network |
| **Delivered Direct; Signature Required** | Do not leave in interoffice mail slot. |
| **Dial-in Modem** | A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator. |
| **DLL** | Dynamically Linked Library. A shared program module used by one or more programs, often installed as part of a program installation. If the current version of a DLL is overwritten by a newer or older version, existing programs that relied upon the original version may cease to function or may not function reliably. |
| **Email** | The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Microsoft Outlook. |
| **Encryption** | A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process. |
| **Enterprise Class Teleworker (ECT)** | An end-to-end hardware VPN solution for home worker access to the Priory network. |
| **Envelopes Stamped Confidential** | You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential. |
| **Expunge** | To reliably erase or expunge data on a PC you must use a separate program to overwrite data. Otherwise, the PC's normal erasure routine keeps the data intact until overwritten. |
| **Forwarded email** | Email re-sent from an internal network to an outside point. |
| **Individual Access Controls** | Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On MACs and PCs, this includes using passwords on screensavers. |
| **Information assets** | Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organisation. |
| **Insecure Internet Links** | Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Priory. |
| **IPSec Concentrator** | A device in which VPN connections are terminated. |
| **ISDN** | There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info. |
| **MAC address** | The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network. |
| **Malware** | A wide variety of programs created with the explicit intention of |

| | |
|---|---|
| | performing malicious acts on systems they run on, such as stealing information, hijacking functionality, and attacking other systems. |
| **Network** | A wired or wireless network including indoor and outdoor networks that provide connectivity to corporate services. |
| **Physical Security** | Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. |
| **Private Link** | A Private Link is an electronic communications path that Priory has control over its entire distance. For example, all Priory networks are connected via a private link. A computer with VPN connected via a standard land line via the firewall has established a private link. MPLS lines into colleagues' homes are a private link. Priory also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Priory has established private links with include all announced acquisitions and some short-term temporary links. |
| **Proprietary Encryption** | An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government. |
| **Remote Access** | Any access to the Priory's corporate network through a non-Priory controlled network, device, or medium. |
| **Removable Media** | Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and Blackberrys; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Priory. |
| **Sensitive information** | Information is considered sensitive if it can be damaging to the Priory or its customers' reputation or market standing. |
| **Smartphone/ Blackberry** | Wireless handheld devices which support push e-mail, mobile telephone, text messaging, internet faxing, web browsing and other wireless information services. |
| **Spam** | Unauthorised and/or unsolicited electronic mass mailings. |
| **Unauthorised Disclosure** | The intentional or unintentional revealing of restricted information to people, both inside and outside the Priory, who do not have a need to know that information. |
| **Virus warning** | Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. |
| **Workstation** | Include: laptops, desktops, Blackberrys and authorised home workstations accessing the Priory network. |

## 28 REFERENCES

28.1 Data Protection Act 1998
Computer Misuse Act 1990
HIPAA Security Rule - Standard 164.310(c) Workstation Security

**Associated Forms:**
None