## Table of Contents

<table>
<thead>
<tr>
<th>Policy Number</th>
<th>Section</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-001</td>
<td>Technology</td>
<td>Computer Security and Confidentiality</td>
</tr>
<tr>
<td>11-002</td>
<td></td>
<td>File Back-Up and Off Site Storage</td>
</tr>
<tr>
<td>11-003</td>
<td></td>
<td>Acceptable Computer Usage</td>
</tr>
<tr>
<td>11-004</td>
<td></td>
<td>Internet Usage</td>
</tr>
<tr>
<td>11-005</td>
<td></td>
<td>Social Media Policy</td>
</tr>
</tbody>
</table>
Policy

Computers owned by and used at Immacolata Manor shall be secured in such a way as to maintain confidentiality of information as well as security of the hardware.

Procedure:

General Safeguards
1. Each employee using a Manor-owned computer shall have a password-protected log-on to the computer and log-on to clear the screensaver for that computer. The screen-saver delay shall be three (3) minutes. Employees are discouraged from recording the password in writing. At no time shall an employee give another employee his/her password with the exception of the Director of Finance and Human Resources and Executive Assistant or designee. All passwords, and any changes to passwords, must be submitted to the Business Manager Director of Finance and Human Resources and Executive Assistant for agency record keeping.

2. Computers shall be placed so that the screen is not easily viewable from the office door or by someone in the office.

3. Employees shall shut down their computers at the end of the day unless otherwise authorized.

4. The Manor shall provide anti-virus software for all agency-owned computers, whether or not the computer is connected to the Internet.

5. Employees may not install their own software on agency computers without the pre-authorization of the Business Manager Director of Finance and Human Resources.

6. Employees who take work home are responsible for maintaining the confidentiality and security of the information transported – including, but not limited to, protection during transport, passwords to access any work-related files on the home computer, and security of papers and disks in the home. In order to transfer information by disk from work to home, the employee must have up-to-date anti-virus and firewall protection on his/her home computer or lap-top.

7. Protected Health Information (PHI) shall not be taken from the Manor to the employee’s home without the specific approval of the Executive Director. All items must be returned the following work day.

8. If a computer is deemed obsolete, all agency information shall be removed from the hard drive with software designed for this purpose before the computer is discarded or given away.
E-mail and S-Comm

1. Immacolata Manor reserves the right to review the e-mail of individual employees that have been received or sent on Manor-owned computers.

2. Email is for business use only. Employees will not use email for personal communication.

3. Employees are discouraged from opening attachments from unrecognized senders.

4. Any employee with an e-mail account automatically has the ability to send and receive e-mail on the Internet. Subscriptions to “list services” are discouraged because the large volumes of mail they generate could impair the performance of the Manor’s mail gateway and internal e-mail system.

5. Protected Health Information (PHI) may only be e-mailed to health, legal or state representatives who use computer systems protected by a secured server and organizations that are therefore also responsible for enforcement of HIPAA requirements. In addition, any organization that has a confidentiality agreement with IM would also be approved recipients.

6. Employees will use common sense and courtesy when utilizing the Internet, including being polite and using appropriate language. Employees will not reveal addresses, e-mail addresses, or phone numbers of other employees without their permission. E-mail is not guaranteed to be private.

Approved: September 27, 2004
Revised: January 31, 2006; January 22, 2009; October 25, 2011; February 5, 2013
Effective: September 27, 2004
Section: Technology Policies and Procedures
Policy: File Back-Up and Off Site Storage

Policy Number: 11-002

Policy:
Copies of important information stored on computers at Immacolata Manor shall be stored off site to ensure their maintenance in spite of computer breakdowns, natural disasters, or terrorist acts.

Procedure:

1. Important information stored in the computer shall be saved on the server through “My Computer.” “Important information” is defined as information that would be needed as a part of disaster recovery.

Approved: September 27, 2004
Revised: October 20, 2004; January 31, 2006; January 22, 2009; October 25, 2011
Effective: September 27, 2004

February 5, 2013
Section: Technology Policies and Procedures
Policy: Acceptable Computer Usage for Direct Support Professionals (See 11-01 for Administrative Staff)

Policy Number: 11-003

Policy:
Use of the internet is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of Immacolata Manor (“IM”). The internet is to be used in a manner that is consistent with the organization’s standards of conduct and is part of the normal execution of an employee’s job responsibilities.

Procedure:

1. IM stakes claim on all information generated, replicated, processed and stored by staff during the course of employment. Such information will extend to e-mails and other information stored on either local work stations or IM servers.

2. IM while reserving the right to protect the best interest of the organization will respect individual staff’s privacy by not knowingly reviewing, revealing, monitoring or discussing information residing on Therap network systems, unless otherwise directed by the Executive Director or designee.

3. IM employees are responsible to maintain password security. This extends to any other access code during the course of employment. Passwords should not be written down, stored in a retrieval system nor communicated to anyone within or outside of the organization, with the exception of the Director of Finance and Human Resources or her designee. Passwords should be changed immediately if an employee feels that the integrity of secrecy at any time is in question. In the event that a password change is required, contact a systems administrator immediately.

4. IM employees are only allowed to access the Therap network and links provided within the network only.

5. IM staff are required to access Therap network per each shift.

6. S-Comm (e-mail) accounts provided by IM should not be used for anything other than organization/sanctioned communications. IM will not tolerate S-Comm that:
   - Is illegal, including but not limited to harassment or pornography.
   - Is obscene, defamatory or discriminatory.
   - Is racist, sexist, abusive, insulting, threatening or obscene.
   - Causes disruption of the workplace environment.
   - Causes embarrassment or loss of reputation to IM.
   - Replaces personal opinions as those of the organization.
7. All necessary software and hardware are provided for online documentation purposes in all IM operated facilities. These are included but are not limited to computers and internet connections via a DSL modem and wireless network router.

IM employees are prohibited from unauthorized installation of software or the use of security-defeating technology like USB flash drives and password cracking utilities. Also wireless network routers should not be reset as to gain access with other portable devices not provided by IM such as personal cell phones, computers, PDAs or MP3 players. Any of the above actions will be reviewed as a serious breach of security and appropriate disciplinary actions will be taken.

8. IM reserves the right to exercise rights of employment for any employee who violates this Acceptable Computer Usage policy.

The following can result in immediate dismissal: Accessing pornography, misappropriation of software/hardware, distribution of protected health information, disclosure of information to a third party not constrained by a confidentiality statement or not in the best interest of the organization, impersonating some other person to access Therap network systems, and aiding/abetting a hacker/phreaker/denial of service attack. Written warnings: all others at the discretion of the Executive Director.

Management reserves the right to change this Acceptable Computer Usage policy at anytime, with approval of either the Board Executive Committee or full Board. If at any time there is a disparity between the guidelines as highlighted above, such summary judgment will rely on the sole discretion of the Executive Director.

Approved: May 27, 2010
Revised: February 5, 2013
Effective: May 27, 2010
Section: Technology Policies and Procedures
Policy: Internet Usage for Administrative Personnel

Policy Number: 11-004

Policy: Internet usage shall be for the purpose of researching information applicable to the mission of Immacolata Manor.

Procedures:

1. Virus and Hacker Protection
   A firewall shall protect the Manor’s computers from outside hackers. Anti-virus software shall be installed and kept upgraded on all computers. Virus detection scans shall be routinely performed on LAN servers and employee PCs.

   All e-mail and other files retrieved from the Internet must be checked for viruses by the employee retrieving the file. Anti-virus software is available on all networks for this purpose. Instructions for loading and running the software will be provided to Internet users. If a virus is detected and you need assistance, notify the Business Manager Director of Finance and Human Resources or Executive Assistant immediately.

   Do not divulge credit card numbers to external web sites, without the prior approval of the Business Manager Director of Finance and Human Resources or Executive Director.

2. Internet Usage
   The only purpose of Internet access over the Manor’s network is to enrich Manor business through communication and information. Use of the Internet for personal reasons is not permitted. The Internet is not to be used for personal gain, advertising, personal business enterprise, personal research, or political lobbying. Links to sites on the Internet must be related to the business of Immacolata Manor. Appropriate links might be to medical information, legislative updates, educational material suppliers, etc. Links that would be inappropriate include, but are not limited to, games and user personal-interest areas.

3. Software
   To ensure consistency and adherence to software licensing agreements, all software needed for Internet access will be installed by technicians obtained through the business office. No software downloaded from the Internet or provided by someone else will be installed on agency computers without the prior approval of the Business Manager Director of Finance and Human Resources.

   Employees will observe all copyright laws. It is the responsibility of the employee when downloading files from the Internet to check for copyright or licensing agreements. If in doubt, assume that it is copyrighted and ask your supervisor about following the law if the file is needed.
Section: Technology Policies and Procedures  
Policy: Internet Usage  
Policy Number: 11-004

4. Monitoring Internet Usage
   Upon request by the Executive Director or the Business Manager Director of Finance and Human Resources, a report of individual employee’s Internet activity can be reviewed. Disciplinary actions will be taken, up to termination, against employees visiting pornographic or other inappropriate sites or abusing personal use of the Internet.

Examples of Acceptable Internet Usage:
- Communication with Business Associates
- Researching MR/DD and medical topics
- Communicating with other members of related organizations
- Personal use with Supervisor approval only and on personal time only. All guidelines pertaining to acceptable and unacceptable use also apply to use on personal time.

Examples of Unacceptable Use:
- Personal business enterprise.
- Representing your own opinions as those of Immacolata Manor.
- Sending or posting confidential information or PHI.
- Generating hate mail, harassment, or other unacceptable behavior.
- Opening an e-mail attachment if you do not know the sender.
- Downloading text or graphics without first obtaining permission from the owner of such text or graphics, if required.
- Downloading unauthorized programs from the internet, including screensavers, music, etc.
- Giving Manor e-mail addresses to individuals not related to the Manor.
- Responding to pop-ups. (Pop-ups should be deleted by using the X in the upper right-hand corner)

5. Policy Violation
   Violation of any part of these procedures can be grounds for disciplinary action.

Approved: September 27, 2004
Revised: January 31, 2006; October 25, 2011; December 16, 2014
Effective: September 27, 2004
Section: Technology Policies and Procedures  
Policy: Social Media  
Policy Number: 11-004  

Policy

In accordance with the Mission Statement Immacolata Manor acknowledges that it has a responsibility to "build relationships that inspire trust, mutual respect, and collaboration among our families, staff and community".

Social media has become extremely popular because it allows people to connect in the online world instantly to form relationships for personal and business purposes. It can take many different forms, including internet forums, weblogs, social blogs, podcasts, pictures and video.

Social media is becoming very much a part of the way we communicate with various audiences. Regular use of these channels of communication enables Immacolata Manor to maximize opportunities with dynamic information sources and allow the organization to market itself to a wider and more diverse audience. However, staff and stakeholders’ use of social media can pose risks to Immacolata Manor’s confidential and proprietary information, and reputation, and can jeopardize Immacolata Manor’s compliance with legal obligations.

This social media policy is designed to encourage the appropriate and effective use of social media platforms, as well as provide guidelines for staff/stakeholders to exercise personal responsibility when using social media.

This policy does not form part of any employee’s contract of employment and it may be amended at any time.

Scope of Policy
This policy covers all individuals working at Immacolata Manor at all levels and grades. It also covers all stakeholders of Immacolata Manor and third parties who have access to Immacolata Manor’s electronic communication systems.

Breach of this policy by Immacolata Manor staff may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether Immacolata Manor equipment or facilities are used.

Staff/stakeholders may be required to remove internet postings which are deemed to constitute a breach of this policy.

Social Media Platforms
There is a vast array of platforms that the term ‘social media’ relates to. However, Immacolata Manor has recognized the key channels most beneficial to the organization. These are: Twitter, Facebook, LinkedIn, YouTube, Meetup
Section: Technology Policies and Procedures
Policy: Social Media

Policy Number: 11-004

This policy, however, applies to all forms of social media and all internet postings, including blogs.

It applies to the use of social media for both Immacolata Manor and personal purposes, whether during office hours or otherwise. It applies regardless of whether the social media is accessed using Immacolata Manor IT facilities and equipment or staff/stakeholder’s personal equipment.

Procedure

Purpose of Social Media
When posting media content to social media sites it is helpful to remember the reasons for doing so. When using Immacolata Manor’s social sites the goals should be to:
· Promote Immacolata Manor’s Mission
· Reach a wider, more diverse audience
· Educate, inform and entertain
· Promote special events and fundraising
· Advocacy on behalf of those we serve

Appropriate professional use of social media
Immacolata Manor engages with social media on a professional level. If any Immacolata Manor staff/stakeholders use social media channels they are asked to follow this policy and any other guidelines which are in place to ensure effective and appropriate usage. When using social media:

You will:
· Use appropriate language
· Think before you post any information online
· Ensure that your profile and any content you post are consistent with the professional image you present in respect of your association with Immacolata Manor
· Make it clear in postings that you are speaking on your own behalf. Write in the first person and use a personal email address when communicating via social media

If you disclose your affiliation with Immacolata Manor, you must state that your views do not represent those of Immacolata Manor. For example, you could state, “the views in this posting do not represent the views of Immacolata Manor.”

You will not:
· Upload content deemed disruptive, threatening, abusive, harassing, obscene, libelous or an invasion of another's privacy – this includes text, audio, photographs and video
· Use Immacolata Manor’s name in a derogatory manner or defame or disparage Immacolata Manor
· Upload content deemed confidential by Immacolata Manor
Section: Technology Policies and Procedures
Policy: Social Media
Policy Number: 11-004

- Infringe the intellectual property of any company/individual – this can create liability for you and Immacolata Manor
- Use Immacolata Manor logos, brands, slogans or other trademarks without Immacolata Manor’s prior written consent
- Use inappropriate/irrelevant hashtags on Twitter
- Post personal messages through Immacolata Manor’s pages on any social media platform
- Breach HIPAA requirements (for example, never disclose personal information about a colleague/consumer online)
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements)

Staff/stakeholders should never provide references for other individuals on social or professional networking sites, as such references can be attributed to Immacolata Manor and create legal liability for both the author of the reference and Immacolata Manor.

Social media is very much part of Immacolata Manor’s strategy moving forward and we encourage the professional use of the various channels on a regular basis. However, use of social media while on duty will be limited to a 15 minute break per a 4-hour shift. Administrative staff may be required to use social media to conduct Manor business.

Immacolata Manor does not discourage staff/stakeholders from engaging with social media platforms for personal usage. However, guidelines are in place to ensure they are being used appropriately and are not putting the organization in jeopardy with inappropriate use of personal profiles.

This policy does not apply to staff/stakeholders in their personal use of social media platforms where the staff/stakeholder makes no reference to Immacolata Manor.

Negativity on social media platforms
It is important that social media platforms are monitored for negative comments about Immacolata Manor. If you are aware of negative comments posted on any of our pages, please make sure you speak to the Director of Development to discuss.

All defamatory postings will be removed by Immacolata Manor’s Director of Development at their discretion. Defamatory postings include, but are not limited to, those that are: racist, sexist, threatening, insulting, unlawful and threatening to another’s privacy.

Implementation, Monitoring and Review
Immacolata Manor’s Director of Development is responsible for maintaining an online social presence and analyzing results. This position is also responsible for the implementation and monitoring of this policy.
Section: Technology Policies and Procedures
Policy: Social Media
Policy Number: 11-004

Approved: January 24, 2014
Effective: January 24, 2014