

UAB DEPARTMENT OF PEDIATRICS

Technology Agreement

I. Equipment Policy

1. I will not move any UAB or CH computer equipment within my division, the department, or the UAB campus without coordination and approval from Pediatric Administration.
2. I will route purchasing/installation requests for software/hardware through Administration via e-mail or otherwise to ensure that any special price breaks, etc. can be obtained.
3. I will direct all computer requests to Pediatric Administration.
4. I will not order parts or services from Children's Hospital IS, or any other company without written permission from Pediatric Administration.
5. I understand the purpose of this policy is to decrease computer down time, operate within all state and federal copyright laws, and decrease redundant expenditures.
6. I will not set up or use wireless routers on campus without express permission from Pediatrics Administration and or CHS IT. Wireless routers used at home should be secured if being accessed by departmental laptops.

II. Confidentiality Policy

1. I will abide by any Children's Hospital Electronic Confidentiality Agreement I may sign in order to gain access to the SMS system or any other CH system.
2. I will not disclose any UAB electronic password for any UAB system, nor will I attempt to learn another's password.
3. I will immediately change my password if I believe that another has knowledge of my password, and if I am unable to change my password, I will report to Pediatric Administration immediately.
4. I will change my passwords to systems that have access to PHI on a regular basis. I understand and accept that Centricity EMR passwords are required by the system to be changed every 60 days. I will also change any other passwords that may access PHI or other confidential information at least every 60 days.
5. I will not store Protected Health Information (PHI) on any portable device such as memory sticks, cd's, or zip disks. Any laptop computer that contains PHI must be equipped with a hard-drive or "boot" password. I will not attempt to remove or disable any type of hardware or software password. I will not allow or initiate the disposal of any copier or scanner without consulting with the Peds IT Department.
6. Virtual Private Network (VPN) keys (which allow access to hospital systems) must be kept secure at all times. I will not install or attempt to use a personally owned computer with a Departmental VPN. Only Departmental Machines may access hospital or UAB systems via VPN or otherwise (internet email excluded).
7. I will not allow any vendor, student, sales rep or other individual not expressly permitted, to access departmental computers or computer systems without prior approval from Pediatrics Administration.
8. I understand the purpose of this policy is to protect the confidentiality of all data I access or have potential access to.
9. I acknowledge that I have received and understand the Electronic Mail Statement.

III. Computer Use Policy

1. I am responsible for the backup/maintenance of all data on my workstation which is not backed up to a department server.
2. If I do not know whether the data I am responsible for is backed up to a departmental server, I will immediately contact Pediatric Administration.
3. I understand the purpose of this policy is to provide a clear understanding of my responsibilities with regard to data management and reduce the maintenance of my computer.
4. I will not download or install applications not specifically authorized by Pediatric Administration without prior approval.
5. I have read and understand the Internet Policy Statement.

IV. Platform Policy

1. I have read and understand and understand the Hardware Platform and Operating System/Database Policy Statement.

I agree that I have read, understand, and will comply with the Technology Agreement, the Electronic Mail Privacy Statement, the Internet Policy Statement, the Computer Software Copying Policy in the UAB Handbook, and any other policy related to a UAB system of which I have access.

Signature_____

Date_____

Printed Name_____

DEPARTMENT OF PEDIATRICS
ELECTRONIC MAIL STATEMENT

1. Electronic mail is considered to be a confidential communication between sender and receiver.
2. Although considered a confidential medium by the department, users should use the same judgment in preparing e-mail messages that they use in formal written communications. The ease of saving, forwarding, and printing e-mail messages makes them much more akin to formal letters and memoranda than verbal communications.
3. Confidentiality of e-mail messages will not be guaranteed.
4. Staff who have incidental access to e-mail by virtue of their job responsibilities should not view others' e-mail. When such viewing is unavoidable, e.g., due to system problems or repairs, the content of such e-mail will be treated with absolute confidentiality. Unauthorized disclosure of such information is a serious breach of ethics that may result in disciplinary action or dismissal.
5. Utilization of the Global Address List to send an e-mail to multiple users (mass mailing) for any non-work related purpose is strictly prohibited.
6. Use of e-mail for any type of harassment including, but not limited to, race, sex, religious beliefs, national origin, physical attributes, or sexual preference is prohibited. The user should immediately report such harassment to Pediatric Administration.
7. Any legal or administrative proceeding, originating from within the Department, UA/HSF System, or a court of law, in which electronic mail data, or any data on a workstation or server is requested, will be furnished as directed by UAHSF attorneys.
8. The initiation of unsecured email communications with patients or patients' families that contain Protected Health Information is prohibited. A HIPAA compliant method of emailing (Kryptiq) must be used in order to send PHI.

UAB DEPARTMENT OF PEDIATRICS

INTERNET USE STATEMENT

Philosophy: The internet can be of great benefit on connecting colleagues around the world, collaborating on projects, downloading articles, and various other resources. However, the internet poses two threats to a productive work environment. Virus transmission through the downloading of an executable program can affect not only the end user, but also potentially any user on the same network. Second, rogue programs which adversely affect departmental software and thus make the user's computer incompatible with other users increase everyone's workload. Therefore, the following policy is designed to protect the department while ensuring that the usefulness of the internet is not diminished.

1. Transmission of any corporate credit card account over the internet is prohibited.
2. The department will not be held liable for the transmission of any personal information over the internet including, but not limited to, personal credit card numbers, social security numbers, and any other personal account information. The department strongly discourages the transfer of personal information over the internet.
3. Use of the internet for the public display of material which results in the incidental or overt harassment of another employee is prohibited. The employee should immediately report any such harassment to Pediatric Administration.
4. Programs and or files such as: screen savers, games, toolbars, chat programs, instant messaging programs etc, can and often do contain virus and/or spyware and should not be downloaded or installed. Viruses and spyware can destroy system files and data on computers causing irreparable damage to the operating system.
5. Care should be taken to avoid "questionable" websites as they often upload viruses and spyware upon viewing the page.
6. Individuals should not attempt to alter or stop the "McAfee Virus Shield" application that runs on every departmental machine. This program and its updates protect our network from virus and malware attacks.
7. Use of the internet is a privilege granted by the Division Director to his/her staff. Internet usage may be monitored or restricted should problems arise with frequency or content of material accessed. This decision is based on the discretion of the Executive Administrator and/or Division Director.

UAB DEPARTMENT OF PEDIATRICS

Hardware Platform and Operating System/Database Policy Statement

1. The Department of Pediatrics supports the PC/Intel computer platform and associated network functions with this platform. The associated operating systems the department supports are Microsoft Windows 2000, and MS Windows XP. These are the only platforms which will run current and future Children's Hospital/UAB Patient Management systems, be able to fully utilize both network programs and resources, communicate effectively within the Department, and be supported under the technology budget.
2. Users of other platforms, such as Macintosh, OS/2, and UNIX will be provided limited technical support for e-mail access through the departmental network only. Questions or issues with hardware or operating systems related to non-supported platforms cannot be addressed due to a lack of support personnel trained on those systems.
3. The Department of Pediatrics will not use departmental funds to purchase any computer equipment outside the IBM PC/Intel platform. Faculty with grant funds which allow computer hardware purchases may be approved to buy computer equipment outside the official department platform if reasonable justification is given in writing. The lifespan of the platform is estimated at four years for faculty and five years for staff.
4. Faculty and staff should not create personal or "homegrown" databases in any format without consulting Pediatrics I.T. Data that is not maintained by DOP IT has the potential to become corrupted or lost. Databases that are not backed up by Pediatrics IT cannot be guaranteed in the event of an OS or hardware failure.
5. Faculty members are welcome to continue using non-official OS systems (such as Macintosh or Linux), with the preceding caveats, but they should notify Pediatric Administration of their intent.