DKH DAY KIMBALL HEALTHCARE

# Guest Wireless (WiFi) Acceptable Use Policy

All users of DKH's Internet network (Network) agree to and must comply with this Acceptable Use Policy (AUP). DKH does not exercise editorial control or review over the content of any Web site, electronic mail transmission, paper printout, newsgroup, or other material created or accessible over or through the Network. However, DKH may remove, block, filter, or restrict by any other means any materials that, in DKH's sole discretion, may be illegal, may subject DKH to liability, or which may violate this AUP. DKH may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of this AUP may result in the suspension or termination of either access to the Network and/or DKH account or other actions as detailed below.

The following constitute illustrative violations of this AUP (this list is not exhaustive; other uses may violate the AUP and DKH retains the sole discretion to determine acceptable usage of its Network):

- **Illegal use:** Using the Network to transmit or receive any material (by email, uploading, downloading, posting, or otherwise) that, intentionally or unintentionally, violates any applicable local, state, national or international law, or any rules or regulations promulgated thereunder.
- **Harm to minors:** Using the Network to harm, or attempt to harm, minors in any way.
- **Offensive use:** Using the Network to access any of the following types of sites: gambling sites, auction sites, hate sites, pornographic sites, other sites that encourage illegal activities.
- **Threats**: Using the Network to transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property.
- **Harassment, discrimination or intimidation**: Using the Network to transmit any information or material (by email, uploading, posting, or otherwise) that harasses, discriminates, intimidates or coerces another in any way.
- **Fraudulent activity**: Using the Network to make fraudulent offers to sell or buy products, items, or services or to advance, promote or facilitate any type of financial or other scam such as "pyramid schemes", "Ponzi schemes", unregistered sales of securities, securities fraud and "chain letters."
- **Forgery, impersonation, misidentification**: Adding, removing, modifying or altering identifying network, message, or article header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited.
- **Unsolicited commercial email/Unsolicited bulk email/"Spam":** Using the Network to transmit any unsolicited commercial email or unsolicited bulk email (i.e., "spam"). Activities that have the effect of facilitating unsolicited commercial email or unsolicited bulk email, whether or not that email is commercial in nature, are prohibited. Using deliberately misleading headers in e-mails sent to multiple parties is prohibited.
- **Unauthorized access**: Using the Network to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of DKH's or another entity's computer software or hardware, electronic communications system, or

telecommunications system, whether or not the intrusion results in disruption of service or the corruption or loss of data.

- **Copyright or trademark infringement:** Using the Network to transmit or distribute any material (by email, uploading, posting, or otherwise) that infringes any copyright, trademark, patent, trade secret, or other proprietary rights of any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, and the unauthorized transmittal of copyrighted software.
- **Collection of personal data:** Using the Network to collect, or attempt to collect, personal information about third parties without their knowledge or consent.
- **Reselling the Network services:** Reselling Network services without DKH's authorization.
- **Network disruptions and unfriendly activity**: Using the Network for any activity which adversely affects the ability of other people or systems to use DKH Network or the Internet. This includes excessive consumption of network or system resources, whether intentional or unintentional. This also includes "denial of service" (DoS) attacks against another network host or individual user. Interference with or disruption of other network users, network services or network equipment is prohibited. It is the user's responsibility to ensure that their system is configured, operated, and used in a manner to avoid excessive consumption of network or system resources. It is the user's responsibility to ensure that their system is configured in a safe and secure manner. A user may not, through action or inaction, allow others to use their system for illegal or inappropriate actions. A user may not permit their system, through action or inaction, to be configured in such a way that gives a third party the capability to use their system in an illegal or inappropriate manner.
- **High Volume, Server Hosting, and non-traditional end user activities:** The Network is intended for an end user's periodic limited use of email, instant messaging, browsing the Internet, and other typical end user activities. High volume data transfers, especially sustained high volume data transfers, are prohibited. Hosting a web server, IRC server, or any other server is prohibited. Accordingly, DKH maintains the right to terminate any user's connection following the detection of any high volume data transfer, server hosting, or impermissible end user activity as determined by DKH in its sole discretion.

DKH requests that anyone who believes that there is a violation of this AUP direct the information to: Data Security Officer, 860-928-6541 x2417

If available, please provide the following information for any such suspected violation:

- The IP address used to commit the alleged violation
- The date and time of the alleged violation, including the time zone
- Evidence of the alleged violation

When reporting an issue regarding unsolicited email please provide a copy of the email messages with full headers which typically provides all of the above data. Other situations will require different methods of providing the necessary information.

DKH DAY KIMBALL HEALTHCARE

DKH may take any one or more of the following actions, or other actions not listed, at DKH's sole discretion in response to complaints:

- Issue warnings: written or verbal
- Terminate the user's access to the Network
- Bill the user for administrative costs and/or reactivation charges, with a minimum administrative cost, if assessed, of $250 per incident.
- Recommend legal action to enjoin violations and/or to collect damages, if any, caused by violations.

DKH RESERVES THE CONTINUING RIGHT, WITHOUT PRIOR NOTICE, TO MONITOR, INSPECT, COPY AND STORE ALL ACCESS, ALL USAGE AND ALL ACTIVITY OVER THE NETWORK, INCLUDING SITES VISITED, TIME SPENT ON SITES AND MATERIAL AND INFORMATION TRANSMITTED OR RECEIVED, AND TO TERMINATE, SUSPEND OR RESTRICT ACCESS AT ANY TIME IN ITS SOLE DISCRETION

DKH reserves the right to revise, amend, or modify this AUP, and our other policies, procedures and agreements, at any time and in any manner.

DKH provides public access to the Internet. There are potentially serious security issues with any computer connected to the Internet without appropriate protections in place, whether connections are made through a wireless network, a cable modem, dial-up access or otherwise. These security issues include viruses, worms and other programs that can damage the user's computer as well as attacks on the computer by unauthorized or unwanted third party “hackers”. If the user has unprotected files on the computer, these files may be visible to hackers on the Internet, potentially including parties with criminal intent. Hackers also exploit vulnerabilities in operating systems to damage a user's computer or even a whole company's network, up to and including the destruction or deletion of files or the re-formatting of drives. It is recommended that all users utilize either a personal firewall or Virtual Private Network systems to protect this information. DKH advises all users to consult a security expert to determine whether there are any potential security holes in their computer's configuration.

DKH MAKES NO REPRESENTATIONS, WARRANTIES OR PROMISES OF ANY KIND CONCERNING A USER’S ACCESS TO THE NETWORK. UNDER NO CIRCUMSTANCES WILL DKH BE RESPONSIBLE FOR ANY LOSS (INCLUDING ANY LOSS OF INFORMATION), DAMAGE OR COST RESULTING FROM A USER’S ACCESS.

DKH SPECIFICALLY DISCLAIMS ANY LIABILITY FOR UNAUTHORIZED THIRD-PARTY SECURITY BREACHES OR THE RESULTS THEREOF. EACH USER ACKNOWLEDGES THAT DKH PROVIDES ACCESS TO THE INTERNET AND THE DKH NETWORK ON AN "AS IS" BASIS WITH ALL RISKS INHERENT IN SUCH ACCESS. BY CONNECTING TO THE DKH NETWORK, THE USER ACKNOWLEDGES THE RISKS ASSOCIATED WITH PUBLIC ACCESS TO THE INTERNET AND HEREBY RELEASES AND INDEMNIFIES DKH AND ITS OFFICERS, TRUSTEES AND EMPLOYEES FROM ANY DAMAGES THAT MIGHT OCCUR.