Newberry House
MONTESSORI SCHOOL

INFORMATION TECHNOLOGY ACCEPTABLE USAGE POLICY

1. INTRODUCTION

The information and communication technology (ICT) at Newberry House Montessori School places emphasis on technological access for all members of the NHMS community. As such, it also places a responsibility on all users of this technology.

2. WHY THIS POLICY EXISTS

The ethical issues surrounding ICT are no different to those laid out in the NHMS rules. The purpose of this acceptable usage policy is to reaffirm our acceptance of these rules and to underline how MHMS rules and standards apply to the information and communications network (ICN).
Any individual in the school who makes use of the school equipment is expected to have consideration for the personal and material rights of others.

3. GENERAL PRINCIPLES

3.1. Hardware & Software

3.1.1. The computers are the property of NHMS as a whole and are therefore a shared resource. As such, any form of tampering with hardware (computers, UPS', air conditioners) and software will fall into the category of vandalism.

3.1.2. No user may change any setting on a computer that will have an influence on another user or move the hardware from one location to another. This includes any and all equipment (mouses, speakers, keyboards, printers, card readers, cameras, etc.).

3.1.3. No user may install any software (including screen savers, games, etc.) of any kind on any NHMS computer. All software or hardware installations have to be performed and approved by the IT Manager.

3.1.4. Software that a user has developed him/herself may be stored in the user's home folder, providing it falls into the category of academic software.

3.1.5. No games of any type may be stored or played (Windows games included) on any computer or the network.

All computers connected to the network automatically fall under and are bound by the management practices of the IT Department.

3.2. Network Identification & Implications

3.2.1. Users may not log onto the network using the credentials of any other user. This is considered to be fraudulent.

3.2.2. Users may not supply their login credentials to any other user. Users are to change their password should they suspect that it may have been compromised.

3.2.3. Users are held responsible for all activities performed with their network credentials. This may also have a cost implication should consumables be used by the use of your network credentials.

3.2.4. Using the NHMS ICN to attempt to break into either the NHMS computer system or an off-campus computer system will be dealt with as a disciplinary issue.

3.2.5. Attempting to obtain another user's password or using another person's password is considered a form of theft (such as stealing a key for another person's locker). Interfering in any way with another person's data, reading their files, or deleting their data is seen in the same light as reading personal letters, damaging personal property or stealing.

3.2.6. Taking advantage of a student who has left the room without logging off is seen in the same light as entering their locker without permission, and is considered inappropriate behaviour (Log the user off, please).

3.2.7. The IT department reserves the right to disable a user account should they feel that there is a probability of misuse. In such cases users are to report to the IT office to clarify matters.

3.2.8. Users have the responsibility to report misuse by other users to the IT Department.

3.3. Data storage and Transport

3.3.1. Memory sticks are the preferred method of data transport.

3.3.2. Users are urged to be considerate in their network usage not to take up unnecessary network disk space.

3.3.3. Shared data must be stored in the shared folders created by the IT Department for that specific purpose.

3.3.4. No data is to be stored on local workstations. Any workstation might be formatted and reinstalled without warning at any time.

3.3.5. E-mail is a communication tool and not a data transport method and large attachments will not be relayed.

3.4. Printing & Printers

3.4.1. Printers may only be used for academic purposes.

3.4.2. Care is to be taken when material is printed. Consumables (paper and toner) are not to be wasted. The A4 paper size should always be used to obtain cost effective paper coverage.

3.4.3. Temporary printouts should be kept to a minimum and page covering should be as high as possible. Small letter sizes are to be used. Web pages, e-mail and photographs are not to be printed. Temporary texts should rather be e-mailed.

3.4.4. Projects should rather be handed in electronically via e-mail to staff or saved into a specific folder especially created for this purpose. Arrange this with the relevant staff member.

3.4.5. No other paper sizes, paper weights (thickness) or other material may be put into printers without consultation with the IT department first.

3.4.6. Scanners and laser printers are not to be used as photocopy or duplication facilities.

3.4.7. Used paper (even if nothing is printed on it) may NEVER be put back into printers.

3.4.8. Paper trays may not be handled by users and paper may not be removed from the trays.

3.4.9. Printers are only to be handled (opened, loaded with paper) by users authorised by the IT Department to do so.

3.5. Electronic Communication (E-Mail, Social Media, Messaging, Blogging, Bulletin Boards & Chat Groups)

NHMS treats e-mail the same as paper mail. Therefore:

3.5.1. Users must respect the privacy of e-mail messages, and mail may not be read by another person or forwarded to another person without permission of the sender.

3.5.2. Electronic mail may not be misused. The following examples are considered as misuse: harassment of other users; unacceptable language;, offensive messages; mail-bombs; mass mail; hate mail, junk mail; sending or distributing games; pornography including pornography considered as art; personal graphic images; chain letters; hoaxes; and anonymous mail.

3.5.3. Sending of e-mail to groups or lists of people (mass mail) is not allowed.

3.5.4. Users may not send a message using another user's network credentials as this is considered to be fraudulent.

3.5.5. The content of a user's home folder and mail boxes is considered private. The IT Department reserves the right to inspect any and all storage spaces for virus infected files as well as unwanted files, to remove them if found, and log and report the matter.

3.5.6. No form of electronic pop-up messaging may be used on the network. This includes using messaging software that forms part of any installation.

3.5.7. Messages posted publicly must not include personal attacks (flaming), and should follow the ordinary rules of appropriate public language.

3.5.8. Any transmitted text to a public environment may not contain any language or content which the author would not be willing to share from the podium at a school meeting.

3.5.9. Various websites considered "non-academic", not age appropriate or "a threat to healthy teenage development" will be inaccessible at NHMS.

3.5.10. Users are strongly encouraged to use a private e-mailbox (Gmail, Live, Yahoo, Hotmail) for private e-mail.

3.5.11. Users are to refrain from attacking the school, staff or students on public websites, chat groups or posting any material on a website without the permission of the person or entity involved.

3.6. Pirated Software

3.6.1. Commercial software is copyrighted and each purchaser must abide by the licensing agreement published with the software.

3.6.2. Use of illegally obtained software will be handled as a disciplinary matter as it falls into the category of theft.

3.6.3. No copyrighted software, music or videos of any nature may be downloaded from the Internet and placed on the computer's hard drive or the network drives.

3.7. Information from the Internet

3.7.1. Access to the Internet is for academic/work related purposes only.

3.7.2. Students may not obtain material that is labelled as not intended for minors.

3.7.3. Users may not download, make public or intentionally view any material that is pornographic, abusive or age inappropriate within the context of the school.

3.7.4. Disseminating the internet addresses (using proxies as an example) of sites containing such material can also be cause for disciplinary action.

3.7.5. If you are in doubt as to whether something falls into the categories mentioned above, please consult with the IT department.

3.7.6. Students may not download any programmes (software) from the Internet. If there is a good reason for obtaining a piece of software, permission must first be obtained from the IT department.

3.7.7. The Internet should be used responsibly. No download larger than 5Mb should be attempted during School hours.

3.7.8. Streaming video should be downloaded and saved for reuse instead of accessing it continuously via the internet.

4. PROCEDURES

4.1. Safety

4.1.1. It is important never to supply personal information (residential address, phone number, etc.) over the Internet to someone you do not know.

4.1.2. Do not open any e-mail or e-mail attachments from an unknown sender. These are to be deleted on reception.

4.2. Connecting personal Laptops\Workstations to the ICN

4.2.1. Any private hardware (Laptops, PDAs, Smart Phones, Desktops) may only be connected to the network if it is in no way a threat to the integrity of the network as a whole.

4.2.2. The school is not under any obligation to install a network point to enable connectivity or to supply a wireless access point.

4.2.3. Computers have to have valid and updated virus software installed. The virus definitions have to be kept up to date automatically on a daily basis.

4.2.4. It is the responsibility of the owner of the device to research how to connect the device to the wireless signals around the campus.

4.3. Consequences

4.3.1. The violation of NHMS rules concerning the use of the ICN will result in the same disciplinary actions that would result from similar violations in other areas of school life.

4.3.2. Misuse of the ICN may result in the loss of privileges such as restrictions on network access, limited use of the computer facilities, or total restriction from the network.

DISCLAIMER:

Newberry House Montessori School does not accept responsibility for data loss of users although all possible steps will be taken to prevent such an occurrence.

Newberry House Montessori School, Board and Staff cannot be held responsible for unacceptable material being viewed or accessed by users. Such cases will, however, be investigated and appropriate disciplinary action taken.

Policy prepared by	Waterstone Governance	August 2016
Approved by Board/Management		
Policy published		
Next date of review		August 2018