PARENTS AND PUPILS

UNITED HERZLIA SCHOOLS (UHS)

INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SOCIAL MEDIA POLICY

TABLE OF CONTENTS

1 INTRODUCTION 2

2 OBJECTIVE AND APPLICATION 2

3 USEFUL TERMINOLOGY 2

4 ACCEPTABLE USE 3

5 CYBERBULLYING 4

6 SOCIAL MEDIA 6

7 PERSONAL DEVICES 8

8 STORAGE OF DOCUMENTS 9

9 MONITORING 9

10 DISCIPLINARY PROCESS 10

PLEASE TO PAY SPECIAL ATTENTION TO THE TERMS HIGHLIGHTED IN BOLD

1 INTRODUCTION

1.1 The advantages of using Information and Communication Technologies for education far outweigh the disadvantages. In order to protect our children and the school, use of ICT must be managed thoughtfully and responsibly so as to ensure that our children have a positive and safe experience and understand the implications of irresponsible use.

1.2 Ethical use of ICT is a key aspect of education. Building the culture of responsibility, accountability and humanity in our schools also has application in the information age. Pupils are, on the whole, proficient users of technology but are not necessarily worldly wise; it is for this reason guidelines are necessary.

2 OBJECTIVE AND APPLICATION

The objective of the Policy is to –

2.1 set out principles and rules that govern use of the ICT System and Personal Devices;

2.2 create and maintain awareness around use of ICT;

2.3 protect UHS and pupils against any action that could adversely affect UHS and/or pupils including legal exposure;

2.4 set out rules for monitoring use of the ICT Systems, Communications and Personal Devices;

2.5 set out consequences of non-compliance with the Policy.

3 USEFUL TERMINOLOGY

3.1 **“Communications**" includes all communications, information and messages (including videos, images, voice, emails) transferred via and/or stored on the ICT Systems and Personal Devices;

3.2 “**ICT**” - Information and Communication Technologies;

3.3 "**ICT Systems**" includes the UHS local area networks and wide area network, the UHS Wi-Fi and telecommunication systems, UHS issued telephones, hardware (including key boards, screens, keyboards, mouse), mobile and smart phones, fax machines, computers (desktop and laptop), tablet computers, as well as the applications running on and services provided by these systems including e-mails and access to the internet and Intranet, and file storage facilities, and other external storage devices;

3.4 "**Personal Devices**" – means personal electronic devices that are transportable by nature and include mobile phones, cameras, video recorders, laptops and tablet computers.

4 ACCEPTABLE USE

4.1 The ICT System is a shared resource and is the property of UHS.

4.2 The ICT System may only be used for the education of pupils and must be used in a responsible, ethical and lawful manner.

4.3 Herzlia Gmail accounts

4.3.1 All pupils from Grade 3 upwards are issued with their own Herzlia Gmail account and password. These accounts, created in the domain "@herzlia.com" are for education purposes only and not personal communications.

4.3.2 **The UHS IT Department and administrators are able to monitor use of the Gmail accounts.**

4.3.3 Pupils may not change school issued passwords. Should a pupil change his/her password, the school may close the Gmail account.

4.4 In using the ICT System and Personal Devices, always have consideration for the privacy of others.

4.5 Use of the ICT System must not affect the functioning of the ICT System, such as by causing system failures, server disruptions or crashes and/or excess use of bandwidth.

4.6 You may not use the ICT System -

4.6.1 in a manner which may adversely affect the dignity of any person, including material that is racist, sexist, pornographic/sexually explicit, obscene, defamatory, intimidating, inflammatory, offensive, demeaning, or a form of "hate speech" or harassment;

4.6.2 in the carrying on of any unlawful activity, whether directly or as an accessory, including online gambling, pirating music, videos and/or software;

4.6.3 in a manner that affects the reputation of UHS, any member of the UHS Executive Committee, any teacher, pupil , parent or guardian;

4.6.4 for plagiarism and copyright infringements. Credit must always be given to the source of information;

4.6.5 to spread computer viruses or hack into any third party systems or communications;

4.6.6 to distribute private information about others or themselves (please refer to the UHS Privacy Policy).

4.7 **Do not –**

4.7.1 tamper with any component of the UHS ICT System;

4.7.2 change any settings or move any component of the ICT System without the prior written consent of the computer teacher or IT technical support staff

4.7.3 use an email account or logon other than your own;

4.7.4 record or take videos of any person on school premises or any school activities without such person's express permission, or the express permission of the school authorities;

4.7.5 share your passwords with anyone other your parent/guardian. If you do and your account is used in contravention of this policy, you will be responsible for any consequences that may arise from any activity conducted via your account;

4.7.6 install unregistered/unlicensed software on the ICT System. Software of this nature includes packaged programs, screen savers, video files, shareware etc.

4.7.7 open any email or attachment from an unknown sender as these attachments may contain a virus. Always check with the computer teacher or IT technical support staff before opening any such attachments.

5 CYBERBULLYING

[To be read with UHS Anti-Bullying Policy]

5.1 Cyberbullying is the process of using the Internet or mobile devices to send and post any text or images intended to hurt, torment, threaten, embarrass another person and includes any such conduct by way of email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms.

5.2 Cyberbullying takes various forms including –

5.2.1 **Instant Messaging (IM)/Text Messaging Harassment:** sending hateful or threatening messages to the target/s.

5.2.2 **Warning wars:** reporting of provoked violations of Internet service providers' terms/website terms which can result in the target being banned from a particular website or social network.

5.2.3 **Text wars or text attacks:** ganging up on the target, including sending multiple text-messages to the victim's cell phone/email .

5.2.4 **Stealing passwords:** masquerading as such a person and then posting inappropriate/harmful/illegal posts via such fake profile.

5.2.5 **Sending/posting degrading** pictures or videos

5.2.6 **Outing**: sharing someone's secrets or embarrassing information online

5.2.7 **Trickery**: tricking the target into revealing secrets or embarrassing information and then sharing it online

5.2.8 **Excluding**: intentionally and maliciously excluding someone from an online or mobile device broadcast group.

5.2.9 **Threatening** the target with personal violence (including death threats) which may inspire fear or a belief in the victim that such personal violence is to take place.

5.2.10 **Cyberstalking**: reported and intense harassment, denigration and threats.

5.2.11 **Internet Polling/Rating:** Who's Hot? Who's Not? Who is the biggest nerd in the sixth grade? These types of questions run rampant on the Internet polls, all created by young people/children.

5.2.12 Posting **real or doctored images of the target.**

5.2.13 **Sharing personal or intimate information about the target;**

5.2.14 **Sharing contact information** about the target coupled with a lewd solicitation ("for a good time call …" or "I am interested in [fill in the blank] …")

5.2.15 **Sending Porn and Other Junk E-Mail and IMs:** Often cyberbullies will sign their victims up for e-mailing and IM marketing lists, especially to porn sites, resulting in the victim receiving multiple e-mails from porn sites.

5.3 Role of the School

5.3.1 **UHS strives to create a climate in which every pupil can develop academically, socially, spiritually and emotionally. In order for this to**

happen, pupils need to feel safe and supported, which includes UHS dealing with all elements of cyberbullying.

5.3.2 **To further such principles, UHS has the right to deal with any incident of cyberbullying when it occurs via the ICT Systems or Personal Devices when linked to the school Wi-Fi.**

5.3.3 **UHS is entitled to a deal with any incident of cyberbullying where:**

5.3.3.1 **cyberbullying takes place off campus or not via the ICT System where the cyberbully/perpetrator is harming/negatively affecting the target's education/schooling or is disrupting learning in the classroom. For example: a pupil cannot concentrate at school, is increasingly absent from school or results in fights at school/in the classroom;**

5.3.3.2 **it impacts on the reputation or integrity of UHS; an employee, pupil or parent**

5.3.3.3 **a pupil confides in a teacher/another pupil about cyberbullying off campus or not via the ICT System and the teacher/other pupil is concerned that such cyberbullying is harming the pupil.**

6 SOCIAL MEDIA

6.1 Social Media are the platforms that allow for interactive participation by users to create content and comment (one to one, one to many and many to many). Such communications can take place via any number of devices, such as computers, tables, smartphones etc. Examples include Facebook, Twitter, Instagram, Mixit, Google+, Tumblr etc.

6.2 **Some examples:**

6.2.1 Blogs - Short for "web-logs", these are sites that can function as on-going journals with multiple entries. Online forums allow members to hold conversations by posting messages. Typically, entries are categorized with "tags" for easy searching. Most blogs allow for reader comments. Examples: Blogger, WordPress, Type Pad.

6.2.2 Micro-blogs - These blogs allow for shorter content posts, typically with a limited set of typed characters allowed. Micro-blogs can be used for status updates and to communicate information to "friends" or "followers" quickly. These are pushed out to anyone subscribed to receive the updates. Examples: Twitter, Tumblr.

6.2.3 Content communities / Media sharing – Services that allow you to upload and share various media, such as pictures and video. For example: YouTube, Flickr.

6.2.4 Bookmarking sites – Services that allow you to save, organise and manage links to various websites and resources around the internet. Example: Delicious, StumbleUpon, Pinterest.

6.3 Rules for Using Social Media

6.3.1 Access to Social Media is a privilege and not a right and is permitted at the sole discretion of UHS for pupils over the age of 13.

6.3.2 UHS encourages the use of social networking/media (Twitter, Facebook, etc.) as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

6.3.3 Use good judgment.

6.3.4 Regardless of privacy settings, assume that all of the information you have shared on your social network is public information.

6.3.5 Always treat others in a respectful, positive and considerate manner.

6.3.6 Be responsible and ethical.

6.3.7 Unless you are specifically authorized to represent UHS as a spokesperson, state that the views expressed in your postings, etc. are your own.

6.3.8 Do not publish, post or release information that is considered confidential or private. If it seems confidential, it probably is. Online “conversations” are never private.

6.3.9 Do not disclose your birth date, address, cell phone number on any public website.

6.3.10 To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules, situations, your school and places of after school activities.

6.3.11 NEVER give out or transmit personal information of pupils, teachers, parents,

6.3.12 Do no post pictures/videos/information of any school activities without the consent of UHS.

6.3.13 Do not post pictures/videos/information of any pupil, parent, teacher, visitor to the school without his/her express written consent.

6.3.14 When using social networking sites, comply with their terms and conditions.

6.3.15 Do not post defamatory or malicious comments about UHS, any pupil , parent, teacher or other employee of UHS on any social media platform or via any mobile messaging application;

6.3.16 Do not use UHS name or logos for endorsements.

6.3.17 Do not use the UHS logo or any school images or iconography on personal social media sites.

6.3.18 Do not use the UHS name or logo to promote any cause without prior consent.

7 PERSONAL DEVICES

7.1 The use of personal devices is allowed from Grade 7 for educational purposes as part of the BYOT initiative.

7.2 UHS cannot guarantee that a personal device will link to the UHS Wi-Fi and further that the Wi-Fi will always be available.

7.3 UHS may limit the number of personal devices on the UHS Wi-Fi from time to time. Bandwidth use is to be limited and may be restricted.

7.4 Personal Devices –

7.4.1 may only be used during school time, school excursions, and extra-curricular activities as long as such use complies with this policy and any school specific rules

7.4.2 must be brought to school fully charged. UHS will at its discretion supply cabling and power points. No pupil may unplug any plugs to charge personal devices

7.4.3 must be switched off or set to silent during classroom lessons and all other school activities, such as assemblies, prayers etc. This includes not making or responding to calls, sending or responding to messages (sms, what's app etc), playing games, surfing the Internet, accessing any social networking sites

7.4.4 may not be used during tests, assessments and exams

7.4.5 may not be used to take photos or videos in class rooms (other than with the express permission of the teacher), on campus, in change rooms, toilets or in any situation that may harm, cause embarrassment or defame a pupil, school, staff , visitors to the UHS or parents/guardians

7.4.6 must be clearly marked with the pupil's name. Each pupil is responsible for the security and insurance of his/her personal devices. **UHS is not responsible for any damages to or theft of any personal device**

7.4.7 must be password protected and have location tracking enabled

7.4.8 must be in good working condition and have the most recent anti-virus software installed.

7.5 Pupils may not update mobile apps or any software on his/her personal devices using the UHS Wi-Fi

8 STORAGE OF DOCUMENTS

8.1 Pupils are provided with network locations in which to store documents and these locations are provided solely for storing school-related documents. These locations may not be utilised to store any personal information.

8.2 **In particular, no personal photos, music and video clips may be stored on any part of the ICT System without the approval of UHS.**

9 MONITORING

9.1 **As part of the continuing effort to protect pupils when using the ICT System and personal devices, and to ensure pupils have a positive and safe experience, the user must acknowledge that UHS and its representatives may monitor, access, examine and intercept any communication on or via any component of the UHS ICT System or personal devices, by human or automated means. For such purpose, UHS has installed the VirtueNet software that is designed to monitor each pupil's use of the ICT System, all his/her communications and all usage of personal devices when connected to the UHS Wi-Fi.**

9.2 **Pupils shall have no expectation of privacy when utilising any component of the ICT System.**

9.3 **Pupils shall co-operate with UHS to enable such access, and review, including providing any necessary passwords. Failure to co-operate with UHS in this way may result in disciplinary action being taken.**

9.4 **UHS may from time to time need to appoint external investigators and/or experts for the purposes of conducting forensic and other investigations into unlawful use and/or access to the ICT systems and/or unlawful activities using the ICT Systems. Such external investigators and/or experts may need to access pupils' communications and/or the ICT system. No investigator/expert shall be granted access to any communications and/or ICT systems, except for the sole purpose of conducting an audit/investigation as described/indicated in this clause.**

10 DISCIPLINARY PROCESS

10.1 Breach of this policy may result in disciplinary action. Please refer to the UHS Consolidated Disciplinary Code

10.2 If you think you have breached the policy, please notify a teacher or the ICT support staff immediately so the school can take the proper steps to help minimize the impact it may have.