## IT System User Agreement

### Policy Scope

The School has invested money and other resources in an information technology infrastructure to further the pedagogical and other aims of the School. This document outlines some of the issues and responsibilities which the Student as a user must be aware of, and accept, in their use of these facilities. Each Student is personally responsible for ensuring these investments are protected and shared at all times.

### Individual Privileges

*Access* – The Student will be provided with access to the internet and to appropriate areas of the School local network/intranet. Incidental personal use of these resources is acceptable as long as it does not interfere with use of School facilities for their intended purpose. Access to the internet may be blocked between midnight and 6am.

*Access to the network by computers not owned by the School* – The Student may access the network using a computer that is not owned by the School, provided they adhere to school policies. This includes laptops, mobile phones, tablets and other network enabled devices.

*Training and Support* - Appropriate instruction in the use of the school network, workstations, and software will be made available to the Student. Limited support will be provided to enable the Student to use these personal resources on the School network, although final responsibility and maintenance of the Student's computer rests solely with the Student.

*Data Storage* – The Student may store data files on the School network servers / file shares or on the schools Google platform. The School encourages the responsible use of space on these, and the removal/archive of older material. Personal files should not be stored on the School network. Any files stored on the local hard drives of School computers may be removed when the Student logs out.

*Privacy* - No guarantees can be given for the privacy of files maintained on the School's network. However; System Administrators will not examine the contents of personal documents without the individual's knowledge, except in system emergencies or under unusual circumstances - such as a breach of this policy.

*Use of Peripherals* – The Student will be able to use the provided computer peripherals for work related to the School. If you require any other peripherals to be installed on a School-owned machine, it will first need to be checked by the School IT department.

*Use of Printers* – The Student will be allowed to print within the limit of a quota defined with the pedagogical team per year to be printed on School facilities. Please use these wisely – the Student will not be allowed more.

### Individual Responsibilities

*Access* - Appropriate personal use of School resources is acceptable as long as it does not interfere with the use of School facilities for their intended purpose, and as long as it does not interfere with the Student's studies. Note that personal computers connected to the School network will be required to meet School standards of security and virus protection. If the Student requires network or internet access on a personal machine, it will first need to be checked by the School IT department.

*Adherence to School Policies* - All appropriate policies of UWC East Africa (including the Plagiarism and Harassment Policies) apply to the Student while using School facilities.

*Data Storage* - While every effort will be made to preserve any data the Student places on the network, it is up to the Student to safeguard their information, through "back-ups" on external hard-drives, USB drives etc.

*User Identity and "Logon"* - It is critically important that the Student logs on with their assigned username and password and logs off when they finish their work. This ensures the privacy of the Student's files on the server, networks and applications and safeguards these files and other information from other users. Also, this ensures that other users will not print on the Student's account. Note that the Student is responsible for actions taken by anyone else using the Student's account – passwords are to be protected!

*Exposure to External Information Sources* - The School is not responsible for Internet users and/or content which come from outside the School, any more than the School controls what the Student may see on television or hear on the radio.

*Installing and Downloading Software* - Users should consult with the Systems Administrator if they wish to make any changes to a School-owned computer system.

*Copyright* - Users must respect the legal protection provided by copyright laws for computer programs, data -compilations and for all other works: literary, dramatic, artistic or musical. Non-licensed software is prohibited from use on all School owned computers and the Student agrees not to use the School network to violate copyright law.

*Security of School Computers* - If the Student becomes aware of any inappropriate or suspicious activity which may compromise School data, computers or networks, regardless of the origin, this is to be reported at once to the IT Department. The School depends upon all users to safeguard the School computer systems and confidential data.

**Examples of Prohibited Uses**

The following are considered inappropriate, and may result in consequences, as outlined in this policy. Users are expected to use their own judgment, as the following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

- Impersonation of another user, individual, or organization for any reason (this includes misrepresenting one's ability to speak for the School)
- The Student allowing another person to use their account, password, email, etc. Users will be held responsible for the uses to which their computing accounts are put.
- Unauthorized viewing of or entry into a file, directory, database, server, computer system or network to which the Student does not already have legitimate permission to use/access
- Unauthorized attempted or actual destruction or alteration of data or information

- Attempting in any way to interfere with anyone else's use of their computer, the network or any other IT resource; this includes spamming (sending large volumes of email to a particular user, flooding a link with extraneous information, etc.) and virus propagation.
- Installing or downloading ANY software, or ANY reconfiguration of a School computer without prior permission of the Systems Administrator.
- Sending or replicating chain letters, virus "alerts", or participating in pyramid schemes.
- Using the School computing facilities in any way whatsoever to cheat or assist others to cheat on any exam.
- Viewing or transmitting by any means information which might be reasonably expected to be perceived by the recipient(s) as being threatening, harassing, violent, offensive, pornographic, racist, sexist, etc.
- Downloading or transferring any material (photo, video, music, documents and other) for which the Student does not have the rights (as in authorization / copyrights) to do so.
- Using any Peer-to-Peer (P2P) file transfer software.
- Using the School system for commercial or for-profit activities.

## Consequences

The School is legally obligated to ensure prohibited activities as outlined above do not take place by persons accessing the Internet from computers connected to the UWC East Africa network. Evidence of such activities by the Student may result in:

- suspension or withdrawal of computer services
- internal disciplinary action, including suspension or expulsion

By signing the Contract of Enrolment, the Parents/Guardians and the Student acknowledge that they have read and will abide by the IT System User Agreement.