HILLCREST HIGH SCHOOL

ICT ACCEPTABLE USE POLICY

1. TERMINOLOGY

The term ***user*** refers to both students and staff.

The terms ***student/s*** and ***staff*** are used specifically where there are differences in the policy as it applies to these categories of users.

The term **direct teacher supervision** means that a teacher is present in the venue and actively supervising the work set for the students in his/her charge.

An **unaccompanied** student is one who uses a school computer when a teacher is not present to supervise his/her work in person.

2. INTRODUCTION

This policy document outlines the acceptable use of Hillcrest High School's information, communication and technology (ICT) facilities and applies to all ICT equipment *including* personal devices (i.e. PCs, laptops, tablets, cell phones, digital cameras, video recorders, etc.) while on the school premises or representing the school elsewhere. The purpose of this policy document is to:

- define what is meant by "acceptable use"; and
- make users aware of their role in preventing both accidental and intentional loss of data and the unauthorised disclosure of information.

3. TERMS OF USE

It is expected that all users will treat with respect the ICT equipment and infrastructure which the school community has provided, and appreciate that its use is a privilege, not a right. This privilege can be withdrawn for a period of time as set down in Section 8 of this document.

3.1 Hillcrest High School's ICT facilities are provided to facilitate teaching and learning and the school therefore reserves the right to place reasonable restrictions on their use. These restrictions will vary between students and staff and between normal classes and exam sessions. Restrictions will also be regularly reviewed and changed when necessary to address specific issues and accommodate new technologies. Because the school's ICT facilities are a shared resource, further restrictions may be applied to individual users whose usage is deemed to be excessive, predominantly non work-related, or wasteful.

3.2 The school's ICT facilities may not be used for personal financial gain and users should not expect ICT staff to assist them with tasks that are of a personal (i.e. non work-related) nature. Use of these facilities for personal purposes should be kept to a minimum. The school will not provide storage space and backups for non-school-related data. When discovered, a user will be sent an email notification by a network administrator that this data will be deleted after 48 hours if he / she does not remove it himself / herself within this period.

3.3 All data stored on ICT equipment owned by the school, and all electronic messages sent or received via the school's messaging systems, are considered the property of the school.

3.4 By using the school's ICT facilities, users expressly waive any right of privacy in anything they create, send, receive or store on any institutional or personal device. By accepting this, users consent to allow suitably authorised staff to access and review all materials that they create, send, receive or store on any institutional or personal device, except where school management deems this information to be confidential.

3.5 The school reserves the right to monitor and review users' network and email traffic, internet usage and the content of any files they generate or access, while at the same time respecting the privacy and confidentiality of this information.

3.6 The school reserves the right to inspect any personal device such as a cell phone or tablet and take disciplinary action if it has been used in violation of this **ICT Acceptable Use Policy**.

4. NETWORK SECURITY

All users require their own unique logon credentials to use a school PC, access, create or store data on the school's network, or print to a school printer. These credentials consist of a username and password and are associated with a network account and specific user rights which simultaneously protect the user's data while denying them access to other users' data and restricted software, much like the PIN for an ATM card.

4.1 Users must keep their passwords private and not divulge them to friends, teachers or colleagues. Passwords should be committed to memory. Passwords should never be written down, but a user may find a reminder phrase useful in helping him/her to recall his/her password. If a user suspects that someone may know their password, they should immediately change it.

4.2 Users are not permitted to share their network accounts with other users under any circumstances whatsoever. Users are responsible for their own accounts and will be held solely responsible for any use or misuse thereof and any expenses incurred by its use (e.g. printing and fines). Only one student is allowed per computer unless they are under direct teacher supervision.

4.3 To avoid inadvertent use of their network accounts, users must ensure that they log off properly so that no one else can use their access privileges. Students must never leave PCs or personal devices unattended while they are logged on to the network. Staff must lock their PCs by pressing the CTRL+ALT+DEL keys and then selecting the "Lock " option if they must leave them unattended.

4.4 Unauthorised access to any computer, server, network, app or data - or any attempt at such - is strictly forbidden.

4.5 Students may not enter any student computer venue without the express permission and presence of a member of staff. If they are available, the network administrators are able to supervise unaccompanied students in the Computer Centre, and the librarians can do the same in the Media Centre.

4.6 The Server Room and Staff Computer Room are strictly out of bounds to all students, and classroom and office PCs and laptops reserved for staff use may not be used by students.

4.7 Users should report any irregularities in network access – especially those relating to access privileges – to the network administrators as soon as possible.

4.8 Users must save their work-related files in their **Microsoft OneDrive** or their home folder on their allocated file server, not on the local hard drive of a school PC. Files on local hard drives are never backed up and on shared PCs they are deleted at log off. Data should never be saved to the Desktop.

4.9 Users must not use portable storage devices (e.g. USB flash drives) that they know or suspect are infected with a virus. Our ESET antivirus automatically deletes infected files from these devices.

4.10 Users must not attempt to install software on any school PC – this is the responsibility of the network administrators alone because of the compatibility, licensing and malware issues involved.

5. GENERAL

5.1 Users can access their home folder on their allocated file server via their **S:** drive. This storage location is only accessible from within the school, which is why users should rather use their **Microsoft OneDrive** instead. Users are assigned a fixed S: disk quota. Should a user find their disk quota insufficient for work purposes, they can motivate for an increase.

5.2 Students are not permitted to play games or watch video clips on school PCs other than those of educational value or which are already available on the school network, and then only under direct teacher supervision.

5.3 Users may use portable storage devices (USB flash drives, flash memory cards, external hard drives, etc.), their **Microsoft OneDrive**, or email, to transfer data between home and a school PC.

5.4 Transmission of any material in violation of South African law or Hillcrest High School rules is prohibited. This includes, inter alia, copyrighted material (music, movies, software, games, e-books, scanned copies of printed material, etc.); threatening, obscene or offensive material; and restricted material that the recipient should not have access to.

5.5 No food, drinks or gum are allowed in the student computer venues in the Computer Centre and Media Centre.

5.6 Tampering with ICT equipment is strictly forbidden. This includes switching off equipment which should be powered up, unplugging cables, changing hardware or software settings, or doing anything else that will inconvenience a teacher or another student or prevent them from using the equipment.

5.7 The use of impolite, anti-social, profane, abusive, racist or sexist language in their digital form is prohibited.

5.8 Cyber bullying of any form is unacceptable, whether via email, text messaging, social network sites or other media. Please report any such incidents to the school's Behaviour Management Officer.

5.9 Unaccompanied students are required to present their teacher's QR code permit and their School Notebook at the Computer Centre Help Desk before being allocated a PC for their use.

5.10 Students are automatically charged from their personal **PaperCut** printing account for any printing and photocopying they do, starting with a credit balance provided by the school. Once this credit has been used up, students must buy R10 vouchers to top up their accounts. Printing and photocopying are charged at the following rates per A4 page or part thereof:

- 50 cents for black text and/or black/greyscale imagery;
- R2,50 for any colour content.

5.11 **MS Teams** requires internet access, but the school relies on external providers for its internet services so it cannot guarantee access to the internet. Bandwidth usage varies considerably during the school day, so the school also cannot guarantee a satisfactory service at all times. These disruptions are, however, becoming increasingly rare.

6. CONTROVERSIAL MATERIAL

6.1 It is unwise to assume that material deemed inappropriate by the school can still be stored on personal devices without the possibility of accidental discovery or transmission. It must be assumed that any such material can enter the public domain.

6.2 Users are not permitted to access undesirable sites on the internet. These include sites with pornographic, racial or sexist content, and sites which are blatantly anti-establishment or promulgate extremist views on any sensitive issue that others could find offensive.

6.3 While the school has systems in place to prevent access to it, users may encounter material on the internet which is inappropriate or offensive. It is the responsibility of users to not initiate access to such material, to immediately withdraw from it should they accidentally encounter it, and to report the incident to the network administrators who will then block further access to these sites and clear the user of any possible guilt. Failure to report such sites will make the user accountable when the internet logs are analysed.

6.4 Where a teacher requires that his/her students research a potentially sensitive issue, this must be carried out under that teacher's direct supervision. Unaccompanied students may not carry out this research on their own because other students may take it upon themselves to do the same.

7. PERSONAL DEVICES

7.1 Users bring their personal devices (laptops, tablets, cell phones, etc.) to Hillcrest High School at their own risk, and the school will in no way be held responsible for their damage, loss or theft while they are on the school premises or if they are taken to a school-sponsored activity.

7.2 The owner of a device is solely responsible for its use and any consequences of its misuse. The sharing of personal devices is therefore discouraged.

7.3 ***The use of mobile routers, including setting up a smart phone as a mobile hotspot, is strictly prohibited. This is because these devices interfere with the school's WiFi network.***

7.4 Personal devices must be either on the student's person, in their hands or secured with an owner-provided heavy duty combination lock in one of the lockers made available for this purpose by the school. Students should *never* leave their personal devices in their school bags where they can be more easily stolen, mislaid or damaged. Personal devices belonging to other users may not be used without their owners' permission, and if one is found unattended, it should be handed over to the nearest staff member for safe-keeping.

7.5 Users must familiarise themselves with the security features of their smart phones and make use of these in the event that they are misplaced or stolen. This requires that they know their Google or Apple ID account credentials. Should their phone go missing, these credentials will allow them to possibly track it (if GPS was enabled), make it ring, and/or erase and secure it from a school PC.

7.6 All personal, WiFi-enabled devices have access to our **Moodle** learning management system (LMS) and their owner's on-line Microsoft account. Devices connected to the **HHS-Students** WiFi network are denied access to social, gaming and other websites that may distract students from their school work. Should a student need access to any of these blocked sites, they are at liberty to use their own data bundle for this – subject to the usual restrictions set by their teachers.

7.7 Personal devices must be configured to obtain an IP address automatically. Devices with static IP addresses will not be able to use the school's WiFi network.

7.8 Since a device's WiFi connection takes precedence over its paid data connection, students must ensure that they have their WiFi turned on and connected to the school's WiFi network to access Moodle and their Microsoft account. The school will not be held responsible for charges incurred by using an external data service provider, whether accidentally or intentionally.

7.9 Users are responsible for updating and maintaining their personal devices. Devices running outdated operating systems and/or apps may be unable to access **MS Teams** or the internet via the school's WiFi network.

8. ADMINISTRATIVE PROCEDURES

A system of fees and fines, administered by the ICT Department, has been put in place for student registration and printing and to encourage students using school PCs and infrastructure to conform to this ICT Acceptable Use Policy. Fines are recorded and repeat offenders may be reported to school management for further action to be taken. This system has been found to work very well and we seldom have to impose fines.

8.1 Every student has his/her own network logon credentials consisting of a unique username and a password of his/her choice. Once his/her network account has been enabled for the first time, each student is responsible for remembering his/her own password. To encourage this and reduce avoidable administrative work, a fee of R2 will be levied to have a password reset.

8.2 Under no circumstances whatsoever may network accounts be shared between users. This is a serious breach of network security and each student involved will be fined R10. Their respective network accounts will be enabled for one day at a time at a teacher's request until they have paid their fine.

8.3 Any student caught tampering with the school's ICT equipment will be fined R50 and their network account will be enabled for one day at a time at their request until they have paid their fine. Tampering is defined as deliberately doing something that will inconvenience or disadvantage another user (e.g. disconnecting cables; changing monitor display settings; forcefully rebooting a computer).

8.4 No food, drinks or gum are allowed in the Computer Centre and Media Centre. A student caught chewing or drinking anything in a computer venue will be fined R10 for a first offence and their network account will be enabled for one day at a time at a teacher's request until they have paid their fine. The fines for further infringements will increase by R5 per incident.

8.5 A student may be fined R10 for a first offence and their network account will be enabled for one day at a time at a teacher's request until they have paid their fine. Offences include, inter alia, the playing of games, music or videos, or browsing the internet without the teacher's permission; attempting to install software; and saving games and non-subject-related .exe files on the network. The fines for further infringements will increase by R5 per incident.

8.6 The network account of a repeat offender may be disabled (without the option to have it temporarily re-enabled) until such time as their grade controller/s have investigated these offences and taken additional disciplinary action. This may also apply to offences such as cyber-bullying and deliberately accessing offensive websites.

8.7 Students must present their School Notebook when having their passwords reset or their accounts re-enabled, since the network administrators may not be able to confirm their identity without these. School Notebooks are also required for entry to a computer venue during breaks and after school to help Computer Assistants with their duties.

8.8 Any changes to a user's network account (e.g. resetting a password or re-enabling the account) may take up to 30 minutes to propagate around the network. Until this process is complete, a user may still not be able to use his/her network account and/or MS Teams account.

8.9 Students and teachers must be aware that a network administrator may not always be immediately available to deal with account issues. It is therefore far better to avoid any situation which may lead to a network account being disabled.

Please keep this policy document for your own records and return only the attached

ICT ACCEPTABLE USE POLICY AGREEMENT.

HILLCREST HIGH SCHOOL

ICT ACCEPTABLE USE POLICY AGREEMENT

2026

REG. CLASS: ☐☐☐☐ **ADMIN. NUMBER:** ☐☐☐☐☐

This agreement must be signed by the student and his/her parents/guardians and returned to his/her registrar or the ICT Department in order to have a network account activated for the first time. Parents/guardians are encouraged to contact the appropriate personnel at the school if they require more information about this policy.

STUDENT

I have read and understood the school's **ICT Acceptable Use Policy** document attached herewith, and hereby agree that while using the school's ICT facilities, I will:

- only use the computers for work purposes and *minimal* personal purposes;
- observe all copyright laws, including those relating to computer software;
- respect the rights and privacy of other users;
- report any security lapses that I may discover;
- minimise the application and inform my teacher if I accidentally come across something that is illegal or offensive.

I will not:

- allow anyone else to use my logon credentials or my school network account;
- use another student's logon credentials or tamper with another student's school network account in any way;
- reveal any private information such as another person's address or phone number without their permission;
- attempt to retrieve, view or disseminate any obscene, offensive, pornographic or illegal material;
- send offensive, racist or sexist messages;
- use my school network account to access chat or dating channels on the internet;
- use my school network account for financial gain;
- use my school network account for political purposes;
- attempt to change or tamper with the school's computer network, hardware or software in any way;
- attempt to bypass the school's network security.

I understand that if the school decides I have broken this agreement, I may be temporarily denied use of its ICT facilities for a period of time as set out in Section 8: Administrative Procedures.

_____	_____	_____
Student's First Name and Surname	*Student's Signature*	*Date*

PARENT/GUARDIAN

I have read and understood the school's **ICT Acceptable Use Policy** document attached herewith. I understand that the school's ICT facilities can provide students with valuable learning experiences. I also understand that, although unlikely, it may give access to information that is illegal or offensive. I accept that, while teachers will properly supervise the work they set for their students, protection against exposure to harmful information depends upon responsible use by students. I hereby give permission for the student named above to use the school's ICT facilities. I understand that should the school decide that he/she has broken his/her agreement, he/she may be temporarily denied use of the school's ICT facilities for a period of time as set out in Section 8: Administrative Procedures.

_____	_____	_____
Parent/Guardian's First Name and Surname	*Parent/Guardian's Signature*	*Date*