TAFELBERG SCHOOL

IT POLICY

(Acceptable User Policy)

Implementation date :

____

Mr L E Benecke
Principal

1. INTRODUCTION

Tafelberg School is committed to the use of electronic resources and technology to enhance teaching, learning and administration. Therefore, staff and learners are expected to utilise these resources within the guidelines set forth in the IT Policy.

In providing our extensive IT facilities, our aim is that these are used optimally as an administrative and educational tool only. We should like to emphasize that the computer facilities are intended for serious information research, curriculum planning, lesson planning and presentation, and not for recreational purposes such as playing games, downloading files for personal or private non-academic use, nor for private social media, business or other use.

The IT Policy addresses the ethical and appropriate use of the technology resources provided by the school, the security of our network, and the safety of our staff and learners. We believe in intellectual freedom and access to information, therefore, the ultimate responsibility for a user's actions rests with the user.

All users have the responsibility to use these resources in a responsible, efficient, ethical and legal manner and must be in support of the educational objectives of Tafelberg School.

Transmission of any material in violation of any South African regulation is prohibited.

2. ACCEPTABLE USES

Direct educational purposes endorsed by the school (ie Principal and Head: Academics)
Constructive communication with other appropriate e-mail users

3. UNACCEPTABLE USES

- Change or attempt to change computer / system settings
- Assumes another person's identify or role through deception or without proper authorization.
- Communicates or acts under the guise, name identification, email address, signature of another person without proper authorisation explicitly given by those users.
- Communicates under the guise of an organisation, entity, or unit that you do not have the authority to represent.
- Intentionally seek information on, obtain copies of, or modify e-email, files or passwords belonging to other users.
- Divulge sensitive personal data to which you have access concerning staff, or learners without explicit authorization to do so.
- Use file-sharing programs to obtain copyrighted material such as music, games, DVD's and other protected items without permission of the copyright holder. Pirating of software is a criminal offence.
- Make copies of a licensed computer program to avoid paying additional license fees or to share with other users.
- Violating copyright laws.
- Using inappropriate or threatening language
- Download, store or disseminate obscene or pornographic material.
- Distributing material for commercial purposes.
- Providing political or campaign information.
- Downloading of private, non-educational material using school's internet
- Streaming, watching and or allowing learners to view movies etc during school time – unless it's content is directly related to the curriculum and has been approved by IT Systems Manager and Principal / Deputies.
- Leaving your PC open and leaving the classroom unlocked, thereby presenting learners with opportunity to access your PC and confidential school and personal data and information.

4. NETWORK RULES AND SECURITY

These rules include, but are not limited to, the following:

- You should not reveal your password.
- You should not logon using someone else's login / password
- Use appropriate language – swearing, using vulgarity, or any other abusive language is inappropriate.
- Caution should be used when revealing your personal address, telephone number etc or those of anyone else's across the internet.
- Caution should be used when revealing credit card or current account information across the internet.
- Do not disrupt network functions.
- Do not attempt to gain unauthorised access to system programs or computer equipment. Attempts to access information on any Tafelberg School network components as any other user or to share a password, will result in cancellation of user privileges. If a security problem is identified, notify the Principal. Passwords should be kept private and should be changed on a regular basis.
- Assume all communications and information accessible via the network are private property and copyrighted.

5. DISCLAIMER

As part of your email signature, you are required to have the following disclaimer on every email that you send out:

This e-mail message is privileged and confidential. If you are not the intended recipient please delete and notify the sender. Please note that any views or opinions presented are solely those of the author.

6. SAFE GUARDING INFORMATION

All staff are responsible for safeguarding information located on Tafelberg Shool's computer systems. The responsibilities include but are not limited to:

- Keeping user names and passwords private.
- Storing files in home directories or in shared folders on the network servers.
- Logging off or locking the computer when leaving the computer.

7. SOFTWARE SECURITY MEASURES

It is important that each user only accesses the system using their own unique password to prevent unauthorised access and allow investigations to take place in the event of a problem arising.

- NEVER disclose your password to another colleague.
- NEVER write your password down.
- NEVER use another colleague's password.
- NEVER install any unauthorised software onto Tafelberg School owned PC or Laptop. (including games, etc)
- NEVER leave a laptop/tablet unattended.
- Only software approved by Tafelberg School is allowed to be installed.
- Computer hardware and software and contained information remains the property of the school, even when departing from Tafelberg School

Only software approved by Tafelberg School is allowed to be installed.
The computer hardware and software and contained information remains the property of the school, even after termination of employment.

The installation of unauthorised Software is a *Gross Misconduct* offence and is expressly forbidden for several reasons:

- The risk of importing viruses
- The new software may effect the functioning of existing software.
- You should already have all necessary software installed.

Any member of staff found to have accessed unauthorised files and data held on the system will be subject to disciplinary procedures.
It is the responsibility of all members of staff to ensure that any confidential information they are processing is secure, particularly when the data is stored on a shared network drive.
Should a staff member require software updates or new software tobe updated, they must put a request to the IT Systems Administrator, in writing. The IT Sytems Manager will then obtain permission from the Principal.

8. PHYSICAL SECURITY MEASURES

***Virus checking* –** a computer virus is a malicious programe that can cause damage and disruption to the functioning of our computer system. These are a few simple rules that must be followed to minimise the risk of infecting our computer system :

- ALWAYS – update Virus check programme daily.
- Ensure all external drives / devices are checked by the IT Systems manager before using it on our system.
- Do not open suspect emails – always check with the IT Systems Manager
- Do not open emails or documents which are flagged by the IT Systems Manager.

9. E-MAIL

- Only mail to be used for the purpose of School business.
- Staff must be aware that private e-mails may contain harmful viruses which may cause damage to computers.
- Staff must use acceptable email protocols and language when communicating with learners, parents, WCED officials and public.
- Use recognised service providers only. Use precautionary measures.

10. PRINTING

- The printer is provided as a service and should be used for school-related work only.
- Check your documents using print preview before printing.
- Never print more than one final original. Photocopy if more copies are needed as photocopying is cheaper than desktop laser printing.
- Printing should be kept to a minimum so as not to waste paper. Where possible recycled paper should be used.
- Private printing for learners is not permitted.
- Private printing for teachers must be authorised by the Document Centre, and paid for. All such monies must be properly recorded and paid to the bursar at regular intevals (LTSM budget item).

11. PRIVACY

- The IT hardware and software equipment and systems are the property of the SGB, and all users accept that as such the SGB (or authorised person ie Principal) may at any time without prior notice, request access to the files on any school computer and or laptop.
- The IT Systems administrator may review files and communications to maintain system integrity and ensure users are accessing the system responsibly.

- When the IT Systems Administrator detects any questionable actions on the school IT system, he is to report it immediately to the Principal or one of the Deputy Principals.

12. LAPTOPS

- The laptop is to be placed in a secure environment at all times.
- The laptop must be comprehensively insured.
- Should the computer be stolen by forceable means the insurance will be covered by the school.
- Should the laptop be lost and/ or damaged through negligence the user will be liable for the excess.
- School laptops issued to staff or learners must be returned to the IT manager when they leave the school.

What is negligence:

- Left in motor vehicle overnight.
- Left in moter vehicle while in transit but visible.
- Not securing it at your workstation/classroom.
- Leaving it in the care of other people.
- The loan or use of third parties of school property.
- Transporting the laptop without its assigned carry bag.
- Eating or drinking whilst working on the computers.

13. LEARNERS

There is a separte AUP for learners, which must be enforced by staff, when learners in their care are using school PCs and laptops / devices.

14. THE IT COMMITTEE

- The IT Committee shall consist of a member of staff, IT Administrator as well as a representative from the School's Governing Body. Technical support could also be co-opted.
- The Committee shall meet on a regular basis.

15. IT ADMINISTRATOR RESPONSIBILITIES

- The IT Administrator shall ensure that all the learners as well as staff members and other users are assigned individual user accounts.
- The IT Administrator must ensure that regular backups and downloading of anti-virus is done.
- The IT Administrator shall ensure that the PCs and computer rooms are well maintained.
- The Committee should render assistance whenever possible to other staff members when required.
- If any irregularities or abuse of the facility is discovered, it must be reported to the Administrator, who in turn will report it to the School Principal or Deputy Principal.
- IT manager is to ensure regular maintenance of all systems and repairs are effected timeously.
- Ensure that server room and IT office is clean and neat at all times.