# MALAWI INSTITRUTE OF JOURBALISM

# ICT Policy

**ICT Mission Statement**

To promote media professionalism through training by providing a secure environment to advance learning experience.

**Introduction**

**The significance of Information and Communication Technology**

Information and communication technology (ICT) prepares users to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognize that Information and Communications Technology is an important tool in both the society we live in and in the process of teaching and learning. Students and lecturers use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination.

They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with pupils being able to make informed judgements about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future.

This policy document sets out the Institution's aims, principles and strategies for the delivery of Information and Communication Technology. It forms the basis for the development of ICT at The College over the next five years.

**The aims of the ICT Policy**

The overall aim for Information and Communication Technology is to enrich learning for all pupils and to ensure that teachers develop confidence and competence to use Information and Communication Technology in the effective teaching of their subject.

- Information and communication technology offers opportunities for pupils to develop their ICT capability and understand the importance of information and how to select and prepare it.
- Develop their skills in using hardware and software so as to enable them to manipulate information.
- Develop their ability to apply ICT capability and ICT to support their use of language and communication.
- Explore their attitudes towards ICT, its value for themselves, others and society, and their awareness of its advantages and limitations.
- Develop good Health and Safety attitudes and practice.

**Access to ICT**

**Network access**

Staff and students have access to reliable and standard hardware and software in order to use ICT effectively as a teaching and learning resource, and as a working tool for management and administration.

**Staff issues**

All staff are entitled to training to improve their ICT capability and have a

responsibility to keep abreast of developments in ICT. The ICT Coordinator, the Network Manager and the County ICT support Unit can be contacted to request support and training in the use of ICT.

**Inclusion**

All users, regardless of race or gender, shall have the opportunity to develop ICT capability. The Institute will promote equal opportunities for computer usage and fairness of distribution of ICT resources. Leaners with a computer at home are encouraged to use it for educational benefit and parents are offered advice through the acceptable use agreement about what is appropriate.

The Institute will monitor the level of access to computers at the Institute to ensure no learners are unduly disadvantaged.

**Using ICT can:**

- address user's individual needs
- increase access to the curriculum
- enhance language skills

Staff should structure their teaching materials to match a learning difficulty. If the situation arises, the Institute will endeavour to acquire appropriate resources to suit the specific needs of the users.

- Looking at the work in their individual paper files or notebooks
- Classroom observation

**Data Security**

As part of the data protection act it is expected that the Institute must take suitable steps to ensure that sensitive data about users is not lost. Employees of

the Institute must not put sensitive data (which contains information about a pupils address, contact details etc…) onto a removable memory device (such as a USB pen drive). If data is to be placed onto any removable memory device then the data protection officer for the school (Librarian) must be consulted and, if approved, must be suitably encrypted.

Teaching staff may wish to use an "electronic mark book" to record pupil progress. This could be placed onto a removable memory device as long as the pupils were only identified by name. For example, information on birth date must not be included.

**Acceptable Use**

MIJ provides access to networked computers to support students' academic work.

In summary, users of the school network are prohibited from:

- logging on to the network with another user's account
- creating or sending offensive or harassing materials to others
- altering the settings of school computers or making other changes which render them unusable by others
- tampering physically with the equipment
- installing software without authorization
- hacking into unauthorized areas of the network
- accessing inappropriate websites or trying to circumvent the College filtering system
- attempting to spread viruses via the network
- any form of illegal activity, including software and media piracy

**Use of WEB 2.0 resources**

Students may be encouraged to access the School Moodle site while at home.

**Internet and use of videos**

Internet access and videos are planned to enrich and extend learning activities. However, setting poorly structured 'research' tasks is shown to be counter-productive. Research tasks should be clearly set out with measurable outcomes. The school has acknowledged the need to ensure that all students are responsible and safe users of the Internet and other communication technologies. Although the school offers a safe online environment through filtered internet access we recognize the importance of teaching our students about online safety and their responsibilities when using communication technology.

**Taking and using images of students**

The school has identified three uses for images of students:

1) For administrative purposes. Photographs of students are placed onto SIMS.net to help identify them.
2) For publicity purposes. Photographs of students may be taken and given to the local or national press to illustrate achievements made by them in school.
3) For assessment purposes. Photographs or videos featuring students may be taken as part of the assessment process. These are then sent off to the examination board.

**Sustainability**

Technical support routines and procedures are continuously reviewed and developed to ensure the sustainability of the network infrastructure, hardware and software.

The whole school asset register provides a continuously-updated audit of hardware that facilitates decisions on repair, replacement and development.
The whole school annual budgetary cycle provides the opportunity to identify maintenance, replacement and development needs for ICT infrastructure, network services, technical support, equipment, and software.

Before being disposed of, all ICT equipment is firstly made safe and removed from the schools register of assets and PAT testing register. Hard drives that have been used in administrative computers and those used in curriculum machines are reformatted to wipe all data and stored for possible reuse. It may be necessary to buy software that will guarantee complete erasure of data. Equipment is then stored in a secure location on site until there is a suitable amount for it to be removed by a registered waste removal company who issue a waste disposal receipt. To facilitate this, the school is registered with the Environment Agency as a Generator of Hazardous Waste.

**Copyright and licensing**

The school will only allow use of licensed software on the school network and any stand alone machines owned by the school. The school agrees to respect the intellectual ownership of software as defined by the Copyright Designs and Patents Act 1988 and 1991 European software Directive.

The purpose of this policy is to ensure that the safety and privacy of all users is maintained when using the Internet on equipments. Users are taught to use the facility sensibly and with proper consideration for others.

1. Any images of students will not be labelled with their names and no close up pictures of our students will be available Online.

2. Students and staff should never reveal their personal details, home addresses and telephone numbers, nor those of others, on the web or when in dialogue with other Internet users.

3. All computer accounts (usernames and passwords) are for the use of a single individual, the person for whom the account was approved. Sharing or loaning accounts is strictly prohibited. All actions when an account is in use are the responsibility of the account holder.

4. Use of these facilities to gain unauthorized access to any other account, at this school or any other facility, is expressly prohibited.

5. Any students finding themselves uncomfortable or upset by anything they discover on the Internet will report it to a member of staff immediately.

6. A member of staff has the right to check student's personal disks for viruses and unsuitable material before they will put any work in the users folder on the institute's computer system.

7. Users must agree not to access unsuitable material or inappropriate websites when using the school computer system. Users must act responsibly and use the MIJ computer system for course/school related work only.

8. Users must respect copyright laws and not plagiarise work.

9. The Institute has the authority to disable users, e-mail facilities and Internet access immediately without warning for failure to comply with this policy. The school must be strict in these matters to ensure that any user breaching this agreement is prevented from bringing the school into disrepute and to ensure that the integrity of the school is maintained for the school, its users and staff.

10. Users have a duty to report infringements of this code by others to a member of

staff.

**Safe use of ICT**
**How will Email be managed?**

Electronic mail (email) is simple to use and relatively cheap. However, care needs to be taken that the potential consequences of reading and sending messages, for both the pupil and the school, are appreciated.

Users should be made aware of the appropriate actions to take if they receive unwanted interactions by email. Bullying, abuse or harassment by email should be dealt with in the school's anti-bullying policy. Users should be advised to guard against giving out personal information at all times.

One of the key considerations is reducing the risk of unsolicited attention put on individual pupils from people outside the school. If individual pupil addresses are used there is a risk of people from outside the school contacting pupils direct. A class/teaching group email addressing system gives complete anonymity to pupils, allows teachers to monitor mail and therefore reduces the risk. Care should be taken if allowing pupils to attach files to email messages.

There are concerns regarding the filtering of emails relating to breaches of individuals rights to privacy etc. Filtering and monitoring is used and details of the approach should be included in the school's Acceptable Use Policy.

Email use is a key concern for schools in terms of safety and management. Parental consent should be obtained for pupils to use email. This should be informed consent with parents having access to the school's Acceptable Use Policy.

With developments of the cloud, it is possible to generate email accounts that are available to staff in school and at home. These mail accounts often come with an online storage facility which allows access to documents and other files from a range of internet capable devices. It should be noted that these types of mail systems aren't backed up, so important files or mail should be copied to another secure location. No sensitive materials or files should be hosted on the cloud without due thought to protecting that data.

**How will the school ensure Internet access is appropriate and safe?**

Users at the institute are unlikely to see inappropriate content in books due to selection by publisher and teacher. The Internet is a new communications medium and staff will need to ensure that access is appropriate to the user. Teachers may expect access to watch YouTube or other video streaming sites as part of everyday teaching activities. Such access brings greater freedom and opportunity but also carries greater responsibility for the teacher to ensure that the content is both educationally suitable and appropriate for pupils to view. Protected access will be required for all pupils.

- Screens used by users will be in public view to staff and pupils in the same group.
- Staff will check that the sites selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be responsible for checking that the content of videos streamed or downloaded from YouTube and other video hosting sites are educationally appropriate to the age and maturity of pupils
- Senior staff will monitor and regularly review the effectiveness of access

strategies for electronic communication.

- Senior staff will ensure that occasional checks are made on files to monitor compliance with the school's Electronic Communications Acceptable Use Policy.

**How will complaints be handled?**

Parents, teachers and students should know how to submit a complaint. Prompt action will be required if a complaint is made. The facts of the case will need to be established.

For example it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions may be of a minor or potentially significant nature. Sanctions for irresponsible use will be linked to the school's behaviour/disciplinary policy.

Possible statements:

- Responsibility for handling incidents will be given to a senior member of staff.
- Responsibility for handling incidents will be given to a member of the senior management team.
- If staff or students discover unsuitable sites, the URL (address) and content will be reported to the ICT Unit. The ICT Unit will immediately prevent access to any site considered unsuitable. Where appropriate investigation will be undertaken. As with drugs issues, there may be occasions when the police must be contacted. Where necessary, following discussion with the Institute, early contact will be made to establish the legal position and discuss strategies.
- A user may have electronic communication access or computer access denied for a period.
- Denial of access could include all school work held on the system,

including any examination work.