INSTITUTE FOR EXCELLENCE IN HIGHER EDUCATION

Near Kaliyasot Dam, Kolar Raod, Bhopal, M.P., INDIA

ICT POLICY: 2015-16

Introduction

IT communications are a key part of the running of the college, and so it is necessary that the Institute, its employees and students adhere to certain standards to protect all parties. It must be remembered at all times that our IT systems and associated facilities are provided principally for educational purposes directly connected with the work of the College. We aim to take a fair and consistent approach to IT usage among staff and students, and this policy sets out our rules on what we would deem to be inappropriate use of ICT facilities. It also covers the use of portable equipment, system security, personal use, computer viruses and monitoring. This policy is not contractual but sets out our current rules and procedures for ICT use.

1. Scope

1.1. The Institute network and computing facilities are provided primarily for the educational purposes and while it is appreciated and accepted that they may also be used for other reasons such as communication and recreation, the priority of the Institute is to ensure that this primary function is maintained above all else. The Policy relates to the use of technology, including:

the internet;

- e-mail;
- the Institute's information and communication technology (ICT) services;
- the intranet and institutional network;
- mobile phones with camera facilities, external networks and other photographic or electronic equipment;
- social networking or interactive web sites.

1.2. It applies to the use of any of the above on institutional premises and also any use, whether on or off institute's premises, which affects the welfare of other students or where the culture or reputation of the Institute are put at risk.

2. Policy Aims

2.1. The aims of this Policy are:

• to create awareness of adequate use of ICT amongst the students and staff by the ways of organizing workshops;

• to encourage students to make appropriate use of the educational opportunities presented by access to the Internet and other electronic communication;

• to safeguard and promote the welfare of students by preventing cyberbullying and other forms of abuse;

• to minimize the risk of harm to the assets and reputation of the Institute.

2.2. Cyberbullying is the use of ICT, particularly mobile phones and the Internet deliberately to upset someone else.

2.3. E-safety means limiting the risks that children and young people are exposed to when using technology, so that all technologies are used safely and securely.

3. General Rules and Regulations of the Institute

3.1. This Policy incorporates the general rules and regulations of the Institute as published in it's prospectus time to time.

4. Internet use

4.1. Students and employees must not use the Internet to access, obtain or distribute inappropriate or illegal material. This includes, though is not restricted to:

• Pornography;

• videos and computer games with a certificate rating older than the person possessing them;

• pirated software, music and films;

• Internet should not be used for cyberbullying;

• Interactive or networking websites.

4.2. Staff and students are not allowed to access interactive or networking websites when using Institute's computers or, if using personal laptops or other devices, on school premises outside the permitted times specified by the Institute which are subject to change from time to time.

4.3. In relation to computer use outside the Institute, staff and students will be held personally responsible for all material they have placed on a website and for all material that appears on a website of which they are the account holder.

4.4. Such students will be subject to Institute's discipline if the welfare of other students or the culture or reputation of the Institute are considered by the Director or his/her representative to be placed at risk.

4.5. Permanent exclusion is the likely consequence for any student found to be responsible for material on his or her own or another website that would be a serious breach of the Institute's Rules in any other context.

4.6. The posting of photographic material which in the reasonable opinion of the Director or his/her representative is considered to be offensive on websites such as YouTube, Facebook, etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. This is the position whether the computer used is a Institute's computer or a computer operated elsewhere including the students's home.

5. College ICT Services

5.1. Students must: at all times, act responsibly in the Institute's computer rooms; report any damage to the Institute's computers or other hardware immediately; treat staff in the ICT office with courtesy and respect; and be considerate of other users (when) in Institute's computer rooms. These are primarily areas for study and should be treated as such.

6. Intranet and College network use

6.1. students are responsible for their actions, conduct and behaviour on the internet in the same way as they are responsible during classes or at break time. Use of technology should be safe, responsible and legal.

6.2. Students must read and accept the Institute's policies and not: use the Institute's network, for cyberbullying; or use the Institute's network to distribute or share inappropriate or illegal material.

7. Personal computers (including mp3 players and other devices)

7.1. Personal computers must be registered and have the Institute's up to date and selfupdating antivirus software package installed.

7.2. Automatic system and security updates should be enabled.

7.3. Students must keep their personal computer (including mp3 players and other devices) free of inappropriate and illegal material.

8. Use of mobile phones, networks and cameras

8.1. students must not use any device to access a mobile broadband network in order to bypass the Institute's firewall.

8.2. Students must not use mobile phones during the working day for any purpose including but not limited to texting, phoning, taking still or moving images, checking the time, using Bluetooth, using as a calculator or surfing the internet. However, if very necessary students will be allowed to use cell phones in the identified mobile phone zones.

8.3. Students may not bring mobile phones into examination rooms under any circumstances.

8.4. The Institute does not accept responsibility for the theft, loss of, or damage to, mobile phones brought onto Institute's premises, including phones which have been confiscated or which have been handed over to staff.

8.5. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

9. Inspection and confiscation of devices

9.1. If there are reasonable grounds to believe that inappropriate communications have taken place, the Director/discipline committee will require the relevant mobile phones / cameras to be produced for examination. The usual disciplinary procedures will apply. Students may expect to have mobile phones and/or cameras confiscated if there has been a breach of this policy.

9.2. The use of cameras, mobile phones with camera facilities, hand held consoles, PDAs, laptop computers or other electronic equipment in breach of this Policy may result in confiscation of the equipment until the end of term and the pupil may be permanently banned from bringing any such devices onto Institute's premises.

9.3. If the director has reasonable grounds to suspect that a student's personal computer, mobile phone, mp3 player, camera or any other device contains images, text messages or other material that may constitute evidence of criminal activity he may hand the personal computer, mobile phone, mp3 player, camera or device to the police for examination.

9.4. All students must allow staff access to images stored on mobile phones and/or cameras and must delete images if requested to do so.

10. Sanctions

10.1. Where a student breaches this Policy, the Director/disciplinary committee may apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, permanent exclusion.

10.2. The measures taken will depend on the seriousness of the offence. Normally a verbal warning will be issued for a minor misdemeanour but further sanctions may be taken against those who repeatedly offend or where the nature of the offence is more serious.

10.3. Students (or their parents) may be asked to pay for any significant expenditure, or indemnify any significant liability, incurred by the Institute as a result of the breach.

11. Procedures

11.1. This Policy authorizes the Director to implement and enforce procedures dealing with the following:

• entering into and maintaining a filtered service with the Institute's Internet service provider;

• the purchase and upgrading of appropriate software and support, including in relation to virus detection;

• setting up and maintenance of auto signatures for outgoing e-mails;

• training staff and students in the use of e-mail and the Internet, particularly in the context of this Policy and general rules and regulations of the institute;

• control of physical access to the Institute's computers; and

• supervision and appropriate monitoring of students' use of Institute's e-mail if there are reasonable grounds to suspect that a pupil may be in breach of any part of this Policy.

12. The liability of the Institute

12.1. Unless the Institute is negligent under the terms of this Policy, the Institute accepts no responsibility to the pupil or parents caused by or arising out of a pupil's use of e-mail and the Internet whilst at Institute.

12.2. The Institute does not undertake to provide continuous Internet access. E-mail and website addresses at the College may change from time to time.

13. Monitoring and Review

13.1. All serious e-safety incidents will be logged in the E-Safety Book.

13.2. The ICT Nodal Officer has responsibility for the implementation and annual review of this policy, in consultation with parents, studnets and staff. The ICT Nodal Officer will consider the record of e-safety incidents and new technologies. The ICT Nodal Officer will consider if existing security procedures are adequate.