SHIA ISLAMIC CENTRE
AL-JAAFARIA

# Staff Communication Devices Policy

# Staff Communication Devices Policy

## 1. Context

We believe that all employees have a responsibility to be ethical and efficient in their official or private use (where permitted) of its property and services. This responsibility includes the use of the Internet and E-mail, both of which are services accessed from a computer terminal. This policy recognises:

- Communication devices are provided for business use;
- Every employee has a responsibility to be productive in the use of their work time;
- Employees may need to make use of communication devices for personal purposes;
- There is a reasonable limit to which employer communication devices may be used for personal purposes; and
- Employees should be provided with guidelines that clearly outline their rights on the use of communication devices.

## 2. Legislative Provisions

Anti-Discrimination Act 1977
http://www.ipc.nsw.gov.au/ppip-act

Independent Commission Against Corruption Act 1988
https://www.legislation.nsw.gov.au/#/view/act/1988/35

Industrial Relations Act 1996
https://www.legislation.nsw.gov.au/#/view/act/1996/17

Telecommunications Act 1997
https://www.legislation.gov.au/Details/C2020C00037

## 3. Employee Responsibilities/Rights

3.1 Computer equipped work stations and the services accessible on them are provided to employees for business use to carry out tasks related to your job.

3.2 Your use must be appropriate -- lawful, efficient, proper and ethical.

3.3 Any identified use of equipment or services thought to be inconsistent with our policies will be investigated. Inappropriate use may be subject to disciplinary action and a range of penalties, including termination of employment and/or criminal prosecution.

3.4 It is not acceptable to intentionally create, send or access information that could damage our reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory.

3.5 Inappropriate use includes, but is not limited to, any use of our equipment or services for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.

3.6 It is inappropriate to transmit, communicate or access any material which may discriminate against, harass or vilify colleagues or any member of the public on the grounds of

- Sex;
- Pregnancy;
- Age;
- Race (including colour), nationality Descent or ethnic background:
- Religious background
- Marital status;
- Disability; and
- HIV/AIDS;

You may be individually liable if you aid and abet others who discriminate against, harass or vilify colleagues or any member of the public. (Harassment will be treated in accordance with existing grievance and harassment procedures and may result in disciplinary action).

3.7 You may not intentionally create, transmit, distribute, or store any offensive information, data or material that violates National or State regulations or laws. We reserve the right to audit and remove any illegal material from its computer resources without notice.

3.8 All information, data or files created by you while employed by us are subject to scrutiny. It is important to remember that electronic messages are official documents that are subject to the same laws as any other form of correspondence. They are subject to statutory record keeping requirements and can be subpoenaed or "discovered" during legal processes.

3.9 Messages conveyed by E-mail and through the Internet are capable of being intercepted, traced or recorded by others. Although such practices may be illegal, you should not have an expectation of privacy and must take care with confidential documents.

3.10 Caution must be exercised when entering into on-line purchasing arrangements. As with telephone orders, proper authorisation for purchases must be first obtained. On-line purchases normally involve the use of credit or charge cards, and due regard must be had to conditions regulating their use.

3.11 E-mail is not to be intentionally used for chain letters.

3.12 Limited personal use of the Internet does not extend to intentionally downloading unauthorised software, lengthy files containing picture images, live pictures or graphics. This includes computer games, music files and the

accessing of radio or television stations broadcasting via the Internet. Downloading of such files increases the load on the network and could degrade the service to other staff with a genuine business need to use the Internet. Such files should not be E-mailed to others.

3.13 No form of computer hacking (illegally accessing other computers) is allowed.

3.14 Employees are encouraged to report breaches of this policy to the Principal/CEO. Internet and E-mail use should be consistent with our code of conduct.

3.15 Access to the Internet should be via officially approved mechanisms only. The connection of standalone modems to individual personal computers must be authorised on a case-by-case basis.

3.16 Where a genuine business reason exists that requires access to sites that would be normally regarded as inappropriate, the authorisation of the Principal/CEO is required.

## 4. Principal/CEO Responsibilities/Rights

4.1 The Principal/CEO is responsible for:

- Ensuring that employees are aware of and understand the policy;
- Monitoring and, where necessary, enforcing policies; and
- Providing leadership by example.

4.2 The Principal/CEO has the responsibility of engendering a commitment to the values espoused by this policy and ensuring adequate controls are in place to administer the policy. Controls may include systems for:

- Random audits;
- Appropriate approvals (including delegation of authority);
- Disclosure of usage;
- Maintaining accurate records;
- Monitoring records; and
- Access control (e.g. network firewalls, STD and ISD bars, encryption controllers etc.).

## 5. Record Keeping

Business communications sent electronically become official records, subject to statutory record keeping requirements. Electronic records are subject to the same standards of record keeping that apply to paper records. Some electronic records cannot be maintained in hard copy form without loss of content or meaning and are best maintained in electronic form. Employees need to be conscious of the need to preserve business communications and care should be taken before deleting any electronic business communication.

## 6. Security

Messages conveyed through communication devices can be intercepted, traced or recorded. Although such practices are normally illegal, users cannot have an expectation of privacy. Use of communication devices represents our community language school to the rest of the world. For example, access through an Internet gateway can be readily traced and mobile telephone or radio calls can be intercepted. Employees should be aware that any Internet site visited may keep a record of the visit.

## 7. Unlawful Use of Communications Equipment

7.1 The use of any telecommunications systems to make or send fraudulent, unlawful, or abusive information, calls or messages is prohibited. Employees are to report any threatening, intimidating, or harassing telephone calls or electronic messages to the Principal/CEO.

7.2 Any employee identified as the initiator of fraudulent, unlawful, or abusive calls or messages is subject to disciplinary action and possible criminal prosecution.

7.3 All employees should be aware that it is illegal to record telephone conversations unless authorised under relevant legislation to do so.

## 8. Mobile Telephones

8.1 The guidelines for personal use and travel related use in this policy apply equally to all types of telephones.

8.2 The Principal/CEO has a responsibility to pay particular attention to properly authorising and monitoring the use of mobile telephones and should ensure measures are in place to ensure the following:

- **Business need:** mobile telephones are provided only in circumstances where there is a demonstrated business need;
- **Accountability:** individuals are accountable for all calls from any mobile telephone assigned to them, and are required to certify billing records;
- **Motor vehicle use:** the use of a hand held mobile telephone while driving is an offence under the Motor Traffic Act. Employees must pull off the road and park before using a hand held mobile telephone. NSW public sector agencies will not be responsible for any fines incurred by employees improperly using mobile telephones. Involvement in an accident while using a hand held mobile telephone could negate any insurance claim. The Principal/CEO should authorise the installation of hands-free mobile telephones in employer-owned vehicles where an operational need can be clearly demonstrated. Alternatively, mobile telephones should be linked to a message bank.

- **Security:** employees who are users or custodians of mobile telephones understand that mobile phone calls can be intercepted, and that extra precautions must be taken to secure mobile phones as they are easily stolen (such as activating in-built security features)

## 9. Email

9.1 Email is a business communication and sending it is classed as a business transaction. Sending an E-mail from your network account is similar to sending a letter our letterhead. E-mail transactions should be handled with the normal courtesy, discretion and formality of all other agency communications.

9.2 Files should not be downloaded unless they are work-related and steps need to be taken to ensure that any files (or software) being downloaded are free from viruses. Care also needs to be taken to prevent unauthorised use of copyright material.

## 10. Communication Device Usage Attracting Other Than Local Charge Rates

The Principal/CEO or his/her delegates is required to approve requests for use of employer communication devices which attract other than local use charge rates on a case-by-case basis. Employees may be required to pay for such usage as reflected on system reports and billing statements. The retention of a personal log noting the date and purpose of all such usage is encouraged for audit purposes. When employees are travelling away from their home base the following guidelines apply:

**Overseas.** When on approved overseas travel, employees are expected to meet all private costs in using communication devices from their travelling allowance. The employer will separately meet charges for overseas business usage made at the overseas locality.

**Within Australia**. When on approved travel within Australia involving overnight stopovers, employees may use employer communication devices to place brief calls to their homes or families to communicate safe arrivals and changes in itinerary.

## 11. On-line Purchasing

Employees are urged to exercise caution in entering into on-line purchasing arrangements. As with telephone orders, proper authorisation for purchases must be first obtained. On-line purchases normally involve the use of credit or charge cards, and due regard must be had to conditions regulating their use. The Principal/CEO has the responsibility to ensure that appropriate controls and security are in place before authorising such purchases. All requests and decisions relating to the authorising of such access must be documented and retained to facilitate scrutiny or audit.

## 12. Fee Based and Subscription Services

Access to services that fees should be barred, unless a business need has been identified authorised by the Principal/CEO or delegate. All requests and decisions relating to the authorising of such access must be documented and retained to facilitate scrutiny or audit.

## 13. Working from Home

Our community language school supports work practices that provide greater flexibility in employment arrangements. The growth in the use of communication devices provides opportunities for effective mutually beneficial arrangements involving working from home. Work related costs of communication device usage and rental will be reimbursed to the employee concerned. It is the responsibility of the employee to maintain appropriate records.

## 14. Personal Use of Communication Devices

14.1 Employees using employer communication devices for personal reasons should ensure that such use is infrequent and brief.

14.2 Employees must not use employer communication devices for the purposes of subscribing to and accessing fee-based services that will be for personal use only.

14.3 Employees may not facilitate or permit the use of employer communication devices by persons not authorised by us, unless urgent business or personal circumstances would reasonably require such use.

14.4 Using employer communication devices for activities that might be questionable, criminal, controversial or offensive, such as gambling, accessing chat lines, transmitting inappropriate jokes, sending junk programs, etc, is forbidden and may lead to disciplinary action being taken against the employee concerned.

14.5 Personal use of employer communication devices is not considered private, and employees using these devices do not have the same personal privacy rights as they would using private communication devices. This means employees reasonably suspected of abusing personal use of employer communication devices may be asked to explain such use (which may be monitored as part of our responsibility to implement appropriate control mechanisms).

14.6 Where reasonable to do so, any personal communication should include a disclaimer making it clear the opinions expressed are those of the sender and do not represent our community language school. A standard form of E-mail

disclaimer reads: "Unless explicitly attributed, the opinions expressed in this E-mail are those of the author only and do not represent our official view."