Information Communication Technology Policy

Updated: December 2015 **Next revision date: December 2016**

1. Objectives

1.1. To apply the most efficient and cost effective method of communication.

1.2. To provide information at induction about Information Communication Technology (ICT).

1.3. To ensure that all staff can access such files that may need to be updated or amended.

2. Scope

2.1. To cover all activities carried out by Develop.

2.2. 'Information Technology' embraces computers, telephones, mobile telephones, faxes, photocopiers, scanners, printers, digital cameras, audio recording and all software applications.

3. Key Principles

3.1. Information technology is a vital tool for the business and should be embraced by all staff as an aid to the effective delivery of services to clients and customers. As developments in IT equipment are likely to continue to be rapid, the CEO, in consultation with First Class Business Solutions, will advise the management on advantageous purchases of hardware/software and highlighting training, safety and security issues for the well being of both company and staff.

3.2. Health and Safety

a. The company Health and Safety Policy Document applies to all users of Information Technology (IT) equipment. At induction, staff should be made aware of safety regarding display screens and equipment by the Health and Safety Manager, including the positioning of screens, lighting, seating and recommended length of time that staff can work at the computer.

b. Free eye tests are available to all staff that use computer screens on a regular basis.
c. All staff have responsibility for ensuring that their own work areas are safe and clear of trailing wires.
d. No member of staff should attempt to repair or fix electrical equipment.
e. The Health & Safety Manager will ensure regular checks on all electrical equipment. The Health & Safety Manager will advise on the placing of all equipment to ensure safety in use.
f. Any concerns over equipment should be referred in the first instance to the Line Manager who will then seek further advice, if necessary, from the Health & Safety Manager.

3.3. Security

a. Only authorised software may be introduced and used on company equipment whether used within the office or for home working.
b. No unlicensed software may be introduced or used- a record of all licenses will be kept by KSS.
c. Software must not be copied except by express contractual agreement.
d. Software may only be used for the purposes that are necessary for discharging the responsibilities of the post held within the company.
e. All software must be checked and proved, to be free of harmful effects such as viruses before it is introduced.
f. All staff should ensure that whenever they leave their screen for any length of time when working on sensitive or confidential information, they should log off.
g. Authorised virus protection used is Sophos and in some isolated cases- AVG.

3.4. Data Protection

a. Develop complies with all conditions of the Data Protection Act and has a nominated Data Controller. All staff are required to familiarise themselves with the Company's Data Protection Policy as they affect their own working.
b. Develop has a legal and moral obligation to maintain confidential data and documentation in a safe environment. All confidential information, when the archiving period has elapsed, should either be deleted from the computer or if in paper copy, this should be shredded.

3.5. Training

a. All users will be trained on the use of software necessary for the implementation of their work.
b. Additional ICT training may be provided through the Line Manager and in liaison with the CEO.
c. When staff become aware of new software or techniques, which would improve the effectiveness of Develop, they should bring this to the attention of their Line Manager or CEO.
d. The CEO will identify the most appropriate training courses in discussion with staff, their Line Manager, the company IT trainer and CEO.

3.6. Use of E-mail

a. The use of email is an efficient and cost effective method of communication- staff should ensure that messages do not contain illegal, lewd or offensive materials or language. Bulk emails are not permitted apart from those considered to be necessary for the effective working of the organisation. Staff should ensure that they do not send emails that are defamatory or libellous in nature and could result in legal action being taken against the sender or Develop.
b. Files containing confidential information should not be transferred by email.

3.7. Use of Internet

a. The Internet may be used during normal working hours to support the work of the company e.g. for research, information, contacts or resources. The Internet may be used for personal purposes during lunch breaks or before or after working hours with the permission of the Line Manager.
b. Staff should take care to avoid accessing any material, which might be considered offensive or inappropriate. This would include all racist, sexist, and pornographic sites or sites promoting violence, inappropriate language and/or unlawful content.
c. Staff may not download anything from the internet unless for specific work related purposes connected with the business. On these occasions the CEO should be informed prior to the download taking place.
d. MSN messenger should not be used at work under any circumstances.
e. Facebook and similar networking sites should not be used at work, even during lunchtimes or before or after working hours.
f. The Develop Management reserves the right to monitor an employee's web activity.

3.8. Housekeeping

a. All staff are responsible for the efficient working on their computer which includes backing-up of important files and for clearing the hardware of unnecessary data. All staff will be given a simple guide to help with this task.

3.9. Laptops

a. If staff are issued with an insured laptop computer, the CEO will load the necessary software onto it. Staff are not permitted to load any personal software onto the machine or to allow friends or family to use it. When travelling, employees are required to virus check any disks or pen drives from their laptop before using on the static equipment within the office.

3.10. Home Working

a. All office procedures relating to safety, confidentiality and security also relate to home working. It is the responsibility of the staff to seek advice from the Health & Safety Manager on how to carry out their own risk assessment of their home working conditions. If equipment is required to made the home environment safe, it is the responsibility of the staff to raise this with their Line Manager who will liaise with the Health & Safety Manager.

3.11. Mobile Phones

a. Develop recognises that there are benefits to the organisation of being able to contact staff in the field by mobile telephone and have therefore provided email enabled mobile phones for relevant staff. It will be the responsibility of the individual to ensure safe and appropriate use of mobile phones for company business. Develop will not take responsibility for improper use of phones, including whilst driving.

4. Staff Responsibility

4.1. All individuals involved with the learning programmes, e.g. staff, volunteers, employers, consultants and learners.

4.2. CEO has overall and final responsibility for all matters relating to complaints.

4.3. The day to day management of Develop's Information Communication Technology policy is delegated to the CEO who will ensure that:-

a. Adequate resources are made available to implement this policy.

b. Adequate arrangements are made to bring this policy to the notice of all staff, individuals, sub contractors and visitors.

c. The effectiveness of the policy and its arrangements are reviewed annually during the relevant Strategy Group meeting or more frequently if deemed necessary.

5. Monitoring and Evaluation

5.1. No additional monitoring required because monitoring is through the achievement of each learning programme's targets.

5.2. This policy is liable to full equality impact assessment annually.

6. Supporting Documents

6.1. This policy should be read in conjunction with the following policies and procedures:-

- Archiving Policy
- Copyright Policy
- Data Protection Policy
- Equality & Diversity Policy
- Health & Safety Policy
- Personnel Manual
- Quality Policy
- Staff Development Policy
- Staff Handbook
- Training Policy

Policy signed by CEO: Mark Pike Date: 01/12/2015