ICT Acceptable Use Policy – Learner Edition

Introduction

The use of technology for SBC Training's learners is provided as a learning tool and must be used in the appropriate manner. The policies defined within this document apply to all users who use SBC Training's network resources.

1. Email Usage Policy

1.1 Email Usage Conditions

The facility for learners to send and receive emails during their course of learning is subject to the following conditions:

- All users are responsible for ensuring that their email usage is within the regulations and is ethical and lawful. Email sent must not include defamatory or libellous statements and should not be used for commercial activity. The sending of text or images that contain material of an offensive, indecent or obscene nature is strictly prohibited
- Email shall not be used as a means of sexual harassment. Email shall not be used for sending offensive comments based on an individual's gender, age, sexuality, race, disability or appearance

If you have an email address provided by SBC Training for your learning programme:

- Outgoing Internet email includes an appropriate disclaimer which is automatically added to your email
- It is not our policy to read your emails. The email software may identify emails with specific types of attachments, e.g. Executable, JPEG, and GIF. If there is an abnormal or unacceptable usage, drill down to individual level will be carried out. Whilst users will not be held responsible for the receipt, the source of unwelcome emails will be identified and communication will be sent to the Senior Management of the company from which the email has been sent, informing them that employees are distributing non-business related material of a questionable nature under their organisation name
- Penalties for misuse of email will depend on the seriousness of the offence, and be in accordance with current SBC Training procedures

1.2 Code of Practice to Email Users

Users should adhere to the following guidelines for appropriate use:

- Check your emails regularly
- Be polite.
- Use "reply all" and distribution lists with caution
- Messages should be clearly addressed to those whom an action or response is expected, "cc" or "bcc" should be used for other recipients of the message so as to be clear who the message is mainly aimed at
- Respect privacy and consider this aspect before forwarding messages
- Unsolicited email, especially with an attachment, may contain a virus. If in doubt, delete the email
- If you do not know the sender of an email or it contains information which is irrelevant, then it is best to just delete it

- Do not try to carry out confidential or sensitive tasks or air controversial views on email
- Enter a meaningful 'subject' field
- Unsubscribe from mailing lists when they are no longer required

1.3 Cautionary Notes

The nature of email is such that total confidentiality cannot be guaranteed and users should be aware of the following points about the use of email:

- Copies of email may exist on a backup copy or a remote system even after the author or recipient has deleted the message
- Email may be forwarded by any recipient without the author's consent, although it may not have been the author's intention
- Usernames and passwords should not be disclosed to others
- Once a message is sent, there is no way to retrieve it

2. Internet Usage Policy

2.1 Internet Usage Conditions

- The Internet service is provided to learners and is intended as a learning tool
- SBC Training reserves the right to monitor Internet usage from our systems. If there is abnormal or unacceptable usage further examination at individual level will be carried out
- It is not permitted knowingly to access websites with sexual or pornographic material, or those which promote to encourage racism or any other objectionable material using SBC Training's systems
- All learners are responsible for ensuring that their Internet usage is within the regulations and is ethical and lawful. The downloading of text or images which contain material of an offensive, indecent or obscene nature is prohibited
- The computer systems, networks, facilities, and accounts are owned and operated by SBC Training. The company reserves all rights, including termination of service without notice, to the computer resources that it owns and operates

2.2 Responsibilities of Internet Users

Users must not, without prior approval from ICT (or appropriate manager), utilise any of the following technologies: routing, forwarding, bridging, ARP Proxying, IP masquerading, Network Address Translation (NAT), IP/IPX tunnelling, SOCKS, application layer proxies, SSH, and peer-to-peer (P2P) on any computer connected to the company's network for the purposes of sending data to or receiving data from an externally located machine.

2.3 Downloading

- Any software or files downloaded via the Internet onto the company's equipment may be used only in ways that are consistent with their licences or copyrights

- No user may use SBC's facilities knowingly to download or distribute illegal software or material. Use of the ICT facilities in this manner will result in internal disciplinary and legal proceedings
- No user may use the company's Internet facilities to deliberately propagate any virus

2.4 Auditing

Under the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, **SBC Training reserves the right to monitor and record Internet usage** but may inspect any or all files that are stored on SBC Training's resources to the extent necessary to ensure a compliance with SBC Training's policies. SBC Training reserves the right to do this any time without notice. Users should not have any expectation of privacy as to his or her Internet usage.

3. Health and Safety

For further information on health and safety with regards to computer work stations please ask your trainer/assessor or SBC Training's person responsible for health and safety.

4. Computer Usage Policy

4.1 Computer Usage Conditions

SBC Training allows their learners to use the company's computers to carry out their learning activities. The use of SBC Training's computers is subject to the following conditions:

- Users are prohibited from installing any software, whether licensed or free, without the prior consent of SBC Training
- Users are not permitted to disconnect or connect any devices to the computers which may damage the systems hardware or cause corruption to system software
- The use of personal USB drives (also known as USB keys, pen drives, memory sticks etc.), floppy disks and CDROM/DVDs are permitted. However the user must ensure that the media is clean from viruses before use. If in doubt ask SBC Training to run a check on it beforehand
- Users are strictly prohibited from dismantling or opening a computer
- Support will not be given for any software programs which are not used for learning purposes or not supplied by SBC Training. Learners who use their own personal laptops are responsible for making sure they have up to date virus scanners, and their software (including the Operating System) is patched with security updates
- Learners are entirely responsible for the licensing and use of any software which is installed on personal computers

4.2 Learner Responsibilities

- Learners who access email from personal accounts (such as Hotmail, or Google Mail) must take reasonable action to ensure that any attachments do not contain viruses and are not downloaded to the network or local computer

- Learners who download any files from the internet are responsible for making sure the source of download is reliable and is unlikely to contain any harmful viruses or worms
- Users of SBC Training's computing services must note that although certain materials may be considered legal in their places of origin, it does not prevent the application of UK law if those materials are considered to be illegal under the law in this country. Similarly, material transmitted world-wide is subject to the law of whichever country it is viewed in
- Only use personal data for a business (SBC Training) related purpose
- Ensure that the use of business related personal data is restricted to the minimum and is consistent with the achievement of business purposes
- Contact SBC Training before conducting any activity which involves the collection, storage or display of personal data through SBC Training's computing services
- Ensure that all published facts are accurate
- Ensure that opinions and views expressed in personal home pages or via bulletin boards and social media do not discredit their subjects in any way which could damage their reputation

Learners must not:

- Display any information which enables others to gain unauthorised access to computer material relating to SBC Training (this includes instructions for gaining such access, computer codes or other devices which facilitate unauthorised access)
- Display any information which may lead to any unauthorised modification of SBC Training computer materials (such modification would include activities such as the circulation of 'infected' software or the unauthorised use of a password)
- Display any material which may incite or encourage others to carry out unauthorised access to or modification of SBC Training computer materials
- Make, transmit or store an electronic copy of copyright material on SBC Training's computing services without the permission of the owner
- Use SBC Training's computing services for placing or distributing advertisements relating to any course or business other than those promoting SBC Training's business activities or its own trading operations
- Place links to social media sites and bulletin boards etc. which are likely to publish defamatory materials
- Share or encourage access to materials which SBC Training deems to be obscene, pornographic or excessively violent, through its computing services
- Use SBC Training's computing services to place or share information/posts/images etc. which discriminate or encourage discrimination on grounds of sex, gender, race, sexual orientation, colour, ethnic or national origins or disability. Any such material is **unlawful**. Any such material will also be against SBC Training's Equal Opportunities Policy
- Place links to sites which facilitate any other illegal or improper use

REMEMBER: Penalties for failing to comply with the Internet Usage Policy will depend on the seriousness of the offence, and will be in accordance with current SBC Training procedures. **Any unlawful activity will be reported to the appropriate authorities.**

ICT Acceptable Use Policy – Learner Edition

Guide to Relevant Legislation

Computer Misuse Act 1990

The Computer Misuse Act was introduced in 1990 to secure computer material against unauthorised access or modification. Three categories of criminal offences were established to cover the following conduct:

1. Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer.
   Penalty: Up to six months of imprisonment or up to a £5,000 fine
2. Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking
   Penalty: Up to five years of imprisonment and an unlimited fine
3. Unauthorised modification of computer material which includes:
   i. Intentional and unauthorised destruction of software or data
   ii. The circulation of "infected" materials on-line
   iii. An authorised addition of a password to a data file
   Penalty: Up to five years of imprisonment and an unlimited fine

Copyright, Design and Patents Act 1988

The Copyright, Design and Patents Act 1988 is applicable to all types of creations, including databases, text, graphics and sounds by an author or an artist. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner or any substantive extraction of information from a database which is not authorised by the database owner will be deemed to be an infringement of his/her rights.

The application of the Copyright Act to electronic copying is even stricter than its application to photocopying, since the fair dealing arrangements which usually apply to libraries (i.e. one article per journal for the purposes of research or private study) do not exist for computerised materials.

Some types of infringement give rise to criminal offences, the penalties for which may amount to up to two years' imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by injunction.

GDPR 2018

This replaces the Data Protection Act 1998. It is designed to enable individuals to better control their personal data. "Personal data" is defined as any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

So in many cases online identifiers including IP address, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject.

To be clear there is no distinction between personal data about individuals in their private, public or work roles – the person is the person.

Official Secrets Acts 1911-1989

The Official Secrets Acts 1911-1989 establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an unauthorised disclosure by a Crown Servant or Government contractor. They also cover material which has been legitimately disclosed by a Crown Servant or Government contractor on terms requiring it to be kept confidential or in circumstances in which it might reasonably be expected to be treated as confidential. This means that certain information handled by SBC Training may be covered by the provisions of the Acts, particularly if such information concerns a project specifically commissioned by a Government office.

Defamation Act 1996

Defamation consists of the publication of opinions and untrue statements which adversely affect the reputation of a person or a group of persons. If such a statement is published in a permanent form, as is the case with statements published on the Internet, including messages transmitted by e-mail, an action for libel may be brought against those responsible.

In accordance with the Defamation Act 1996, SBC Training acknowledges the convention of academic freedom, but will take all reasonable care to avoid the dissemination of defamatory material and will act promptly to remove any such material which comes to its attention. Messages which have only one intended recipient may reach a vast audience through the Internet and as a result, the transmission of statements which discredit an identifiable individual or organisation may lead to substantial financial penalties.

Obscene Publications Act 1959
Protection of Children Act 1978
Criminal Justice Act 1988
Sex Discrimination Act 1975
Race Relations Act 1976
Disability Discrimination Act 1995
The Equality Act 2010

The Sex Discrimination Act 1975, the Race Relations Act 1976 and the Disability Discrimination Act 1995 are guided by the principle of prevention of unfair discrimination on the grounds of sex, including discrimination against persons who have undergone gender reassignment, race or disability. The Acts make unfair discrimination a civil offence, and in certain other circumstances the law is supported by criminal sanctions.

Criminal Law

The incitement to commit a crime is a criminal offence in itself, regardless of whether a crime has actually been committed or not. This includes the provision of information via computerised services which facilitates any of the activities which this code has highlighted as criminal offences.

Terrorism Act 2000

An attack on any electronic system can be classed as an act of terrorism as well as a criminal office. What constitutes an attack within the scope of the Act includes hacking websites or blocking websites, with a political agenda or public intimidation in mind.