michaelJohn Academy

COMPANY POLICY

NAME OF POLICY: Student I.T. Systems & Internet Acceptable Use Policy

PURPOSE OF POLICY

1. This policy applies to all students.
2. This policy relates to all Company information technology, communications, networking, Internet, data storage & associated systems. If in doubt, any technology related system should be assumed to fall within this policy unless informed otherwise by a suitably delegated member of the management team.
3. All Company IT systems, software, infrastructure, network access & Internet access are provided solely for business and educational purposes.
4. Personal use is expressly forbidden unless explicit permission has been granted by a suitably delegated member of the management team.

MONITORING

MJA staff members will monitor student computer usage, this is in line with the prevent duty and safeguarding policies.

Technology may be deployed to automatically monitor, filter and block access to Internet sites deemed inappropriate or unrelated to The Company's business.

Technology may be deployed to automatically monitor, filter & alert based on the content, destination or other characteristic of any electronic communication sent from, or passing through, the Company computer or network systems.

LIMITATIONS/ RESTRICTIONS ON USAGE

Personal use of the Internet may not take place at any time during work and college hours unless permitted by a member of staff.

Attempts to browse or gain access to inappropriate sites are **strictly prohibited at all times and will result in disciplinary procedures**. These include, but are not limited to, the following types of sites: adult/sexually explicit, racial/sexual/defamatory, drugs/alcohol misuse, harassment, gambling, games, hacking, extreme political activities or radical ideology.

Internet messages or postings that contain defamatory or similar written attacks are strictly prohibited. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

4.1. No software or files may be downloaded from the Internet and installed on to the Company computers for personal use.

4.2. No software or files may be downloaded from the Internet and installed on to The Company computers for business use without the explicit permission of the delegated member of the management team.

4.3. Detaching/launching attachments from personal web-based mail accounts onto The Company's computers is strictly prohibited.

4.4. Misrepresenting, obscuring, suppressing, replacing a user's identity, or assuming another user's identity on the Internet or any of The Company electronic communications system is forbidden.

4.5. Whenever employees provide an affiliation with The Company on the Internet they must clearly indicate the opinions expressed are their own, and not necessarily those of The Company.

4.6. Employees may not publicly disclose internal Company information via the Internet that may adversely affect The Company's business interests.

4.7. Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, employees must consider whether the posting could put The Company at a competitive disadvantage or whether the material could cause public relations issues. Employees must gain permission from their line manager prior to undertaking such an activity.

4.8. All information taken from the Internet should be considered suspect until confirmed by separate information from another source. Accordingly, before using free Internet-supplied information for business decision-making purposes, employees must corroborate the information by consulting other sources.

4.9. Users may not create networking connections, Internet dial-up or broadband connections on any Company PC system without the express & explicit authorization to do so from a suitable delegated member of the management team or support organisation.

LEGAL RESPONSIBILITIES

Any communication initiated using The Company's facilities may reasonably be construed by the recipient as expressing the views of both the author and The Company alike. Care should therefore be taken to ensure that communications do not:

4.9.1. Provide for, imply, encourage or condone a breach of The Company's Equal Opportunities Policy and any related legislation.

4.9.2. Provide for, imply, encourage or condone a breach of the Computer Misuse Act 1990 or the Data Protection Act 1998.

4.9.3. Create an unintended contractual agreement through the acknowledgement or acceptance of another party's terms and conditions.

4.9.4. Incorporate either the work of a third party for which prior consent to reproduce has not explicitly been received, or graphics, logos or other electronic files/data which are not owned by (or licensed to) The Company.

Users are reminded that emails (or similar electronic communications) must be regarded as any other business correspondence and should be retained for future reference.

SECURITY & PIRACY

1. No software should be installed on Company IT systems without approval from the management team.
2. All software should be legally sourced and installed in accordance with any licensing or volume conditions.
3. Company IT systems may be audited from time to time to ensure compliance with software, firmware & hardware licensing conditions.
4. Students are reminded that installing illegal, unlicensed or 'pirated' software may constitute a criminal offence. Under no circumstances should such software be installed on Company IT systems.
5. The use of software 'crackz', patches & hacks to defeat copyright restrictions, licensing conditions, security features and trialware limitations is specifically forbidden.
6. Students must not knowingly disable anti-virus software installed on Company IT systems.
7. Students must not knowingly disable hardware or software firewall – or similar security systems – installed on Company IT systems.
8. Students may not make configuration changes to any security software or hardware – such as, but not limited to, anti-virus & firewalls – installed as part of the Company IT infrastructure.
9. Users must notify the nominated manager, support person or organisation if any security software notifies the user that it has become out of date, if the protection software notifies the user that a virus has been found or if the protection software notifies the user that a security intrusion/breach has occurred or is in progress.
10. Where a member of students receives automated notification of the presence of a virus they should, in addition to notifying the nominated support person or organisation, cease work on that PC and if possible, disconnect from any internal network.
11. An infected terminal/PC/Server/workstation may not be switched back on (or reconnected to the Company network) until approval is received from the nominated support person or organisation.
12. Care must be exercised at all times to minimise the risk of contracting a virus. Therefore, students must not:
13. Load illegal software (including the running of programs from a remote source)
14. Load software from free diskettes / CD ROMs / Flash Drive / other external storage devices
15. Load legal software unless it is necessary as part of their normal job to do so
16. Connect to bulletin boards or other information sources via a communication link; unless it is necessary as part of their normal job to do so

17. Connect a Company computer to an unprotected customer network
18. Disable protection provided by a customer, or make any changes to a customer's computer that renders the protection inoperative; unless it is necessary as part of their normal job to do so
19. Students may not write, code, dissemble, modify or knowingly transmit any virus, worm, Trojan or similar malicious code.
20. Portable computer equipment is provided to students on the basis that the member of students is responsible for its safe handling and protection against loss. Students are required to ensure that the equipment is kept in good condition, precautions are taken to avoid damage to the equipment and that the equipment is left in a secure location to minimise the chance of loss.
21. Should any member of students fail to observe this policy, The Company may, at its discretion, require the member of students to pay all or part the costs of any repairs to, or replacement of, the equipment.
22. Computer equipment (including portable & handheld computers, PDAs & any related IT hardware/software) must not be left in an unattended vehicle unless absolutely necessary. Where, through necessity, equipment is left, it must be secured in the boot of the vehicle. When in transit, students are required to place computer equipment out of sight (wherever possible) or preferably, secured in the boot of the vehicle.
23. Where portable equipment is to be left in an office location over night, the member of students is required to ensure that it is stored in a suitable secure area.
24. Students must not divulge any log-on identities, passwords or similar security information to any other member of students or third party. Students are reminded that under no circumstances will they legitimately be asked to divulge a system password to anyone other than previously authorised support students.

COMPUTER MISUSE ACT (1990)

1. All students are reminded that The Computer Misuse Act (1990) makes provision for securing computer material against unauthorised access or modification by making the following actions criminal offences:
2. Obtaining or attempting to obtain unauthorised access to any computer program or data held in a computer;
3. Obtaining or attempting to obtain unauthorised access with intent to commit or facilitate the commission of further offences; and
4. Unauthorised modification of the contents of a computer.

Custodial sentences may be given upon conviction of any of these offences

IF IN DOUBT

All users are reminded that this policy forms an important part of their terms & conditions of employment. Breaches of this policy will be regarded as a serious matter & disciplinary action, up to and including dismissal for gross misconduct, may result.

1. If you are unsure about any aspect of this policy or day-to-day IT & Internet operations, please contact the nominated support organisation or individual.
2. Any user subject to harassment, attack, intimidation or in any way concerned about their use of Company IT systems should contact the nominated support organisation or individual for confidential advice.

This policy will be reviewed annually as per the company policy review schedule.

Signed and verified: July 2018

by Data/Compliance Officer:…….

* This policy can be made available in larger type.

VERSION NO 2.