YMCA PLYMOUTH

ELECTRONIC MEDIA POLICY (including security of equipment)

The Electronic Media Policy (EMP) sets out the Association's (wherever mentioned in this policy this also includes Discovery College) conditions for the official and personal use of the internet, intranet, e mail, telephony, PCs and laptops and the need to protect security of equipment.

This policy is designed to safeguard:

- the interests of staff;
- the Associations business and reputation;
- the integrity, performance and availability of our computer systems.

This policy is the definitive guidance for anyone working for, or on behalf of the Association (including being a student at Discovery College). It also applies to people working in and out of our sites, from home or in transit.

Your responsibilities

It is vital you understand the policy. The rules are part of the terms and conditions of employment. Failure to follow the rules is a serious matter. You may have disciplinary action taken against you. The consequence of failing to follow the rules can result in penalties up to and including dismissal. If you commit a criminal offence you may also be prosecuted.

Computer security

Authorisation for access to the Association network is based on the requirements of the individual's job as stipulated in their job description. Those individuals who are required to use the Association's computers to carry out the duties of their role will be issued with a password for an internet and e-mail account. These individuals are entitled to use these facilities for business and limited personal use, details on personal use are covered below.

Employees must not take any equipment off site without the express permission of their Line Manager. On the occasions that this is permitted the employee is responsible for ensuring the security of that equipment. It must be kept securely at all times and never left in vehicles overnight.

Where a staff member has been issued with a laptop, that individual is responsible for its security. It MUST not be left out overnight. It should be stored away safely and wherever possible in a lockable drawer or cabinet.

Failure to comply with this could result in disciplinary action depending on the circumstances involved.

Network Security/Passwords

All users are issued with a password when their user account is set up. Users are responsible for the secure keeping of their password and log in details. Passwords must not be disclosed to other individuals. Users will be held responsible for any breaches of this policy as a result of disclosing their password to a third party. Users are responsible for the security of their terminal and must ensure that it is not used by an unauthorised person. To ensure this is not possible users must ensure that their terminal is 'locked' when they are away from the terminal for any period of time.

USB and CD use

You must not attach any USB device or insert a CD to import or export software or data without prior approval. This is to prevent the possible introduction of viruses.

The Internet

Browsing the internet for personal use is only permitted outside working hours and should be kept to a minimum. Browsing, even for business purposes can be time consuming and wasteful of resources, therefore also should be kept to a minimum.

Logging on to sexually explicit websites, using the Internet for gambling or for any kind of illegal activities is prohibited. Accessing any sites promoting radicalisation or linked to radicalisation are also prohibited (in line with the Prevent Duty).

Using the Association's internet for 'blogging', or any other type of web chat is also considered unacceptable use.

Downloading

Downloading and circulating offensive, obscene or indecent material is strictly forbidden at any time. Offensive material may include sexist, racist, ageist, defamatory or any discriminatory, comments, jokes, stories or statements which might be deemed inappropriate or offensive.

When down loading information from the internet consideration must be given to the Copyright, Designs and Patents Act 1998, which states that only the owner of the copyright is allowed to copy the information. Any copying without permission, including electronic copying, is prohibited.

The copyright laws also apply to software and no software should be downloaded without a license and prior authorisation from the IT lead for the Association.

The Association licences the use of computer software from a variety of outside companies. The Association does not own this software and, unless authorised by the software developer, neither the Association nor any of its employees have the right to reproduce it. To do so constitutes an infringement of copyright. Contravention is a disciplinary matter and will be dealt with in accordance with the Association's disciplinary procedure.

The Association's computer network makes it vulnerable to viruses. Therefore, only duly authorised personnel have the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses by authorised personnel. Any employee found to be contravening this will face disciplinary action under the Association's disciplinary procedure.

Due to the large amount of information available via the internet, which is uncontrolled, care should be taken when obtaining and using information sourced in this manner. Only information from legitimate sources and organisations should be used.

Social Networking

Whether employees use social networking services at home or at work, there is a level of staff conduct and behaviour that the Association has a right to expect. The Association has a valid right to be concerned and take disciplinary action against employee's misconduct both at work and in their personal lives if it leads to a breach of commercial and personal confidentiality or damages the reputation of YMCA Plymouth by slandering the Association, colleagues, members or customers.

If an employee openly criticises their employer online, this can be hugely damaging to the employer's reputation and has the potential to impact customers using our services or funders supporting our programmes especially given the vast number of potential readers on sites such as Facebook.

Any serious misuse of social networking sites that has a negative impact on the Association may be regarded as a disciplinary offence. All staff should be aware that the Association will take seriously any occasions where the social networking services are used inappropriately. If occasions

arise of what might be read to be online bullying or harassment, these will be dealt with in the same way as other such instances.

An employee must not disclose confidential information relating to his/her employment at YMCA Plymouth.

Social networking applications must not be used to publish any content which may result in actions for defamation or discrimination.

Whilst it is acknowledged and respected that employees have a right to a personal life, their behaviour and conduct should not breach reasonable standards of conduct and behaviour.

E-mail

The purpose of these rules is to protect the Association's legal interests. E-mail is not an informal communication tool, but has the same authority as any other communication to and from the organisation.

E-mail must not be used for unsolicited correspondence or marketing campaigns and employees must not commit the Association financially by e-mail unless they have been granted a specific level of delegated authority to do so.

Users are not permitted to spend excessive time 'chatting' by e mail for personal and private purposes during their normal working hours.

The forwarding and sending of offensive e-mail will not be tolerated. Offensive material may include sexist, racist, ageist, defamatory or any discriminatory comments, jokes, stories or statements which the recipient deems inappropriate or offensive. Users who receive this type of inappropriate material from external e-mail addresses should delete the e-mail immediately and notify the sender not to send further e-mails. Alternatively, if a user receives this type of e-mail from an internal e-mail address they should forward the e-mail to The Support Services Director for action to be considered against the sender, under the disciplinary policy and then delete the e-mail from their system.

A reasonable amount of personal e-mails are permitted, however these must not consist of offensive material, be clearly marked 'personal' and only be sent out of normal working hours.

Users are prohibited from using e-mail to circulate any non-business material; this includes 'chain' letters.

Use of instant messaging systems must be expressly approved in advance by the Association.

Only relevant e-mails should be sent, and users should avoid the automatic forwarding of all messages to long circulation lists which unnecessarily increases the traffic and the time spent dealing with irrelevant correspondence.

Wrongly delivered messages should be re-directed to the correct person, if known, the sender be notified and if the e-mail message contains confidential information, use must not be made of that information and nor must it be disclosed.

Disclaimers

Unregulated e-mail access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded e-mail can expose the Association to libel. As such, e-mail to clients and customers must follow the Association's designated house style, which will be supplied to authorised users. Failure to follow house style is a disciplinary matter and will be dealt with under the Association's disciplinary procedure.

Monitoring

The Association reserves the right to monitor employee and student e mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are:

- to promote productivity and efficiency;
- for security reasons;
- to meet 'prevent duties';
- to ensure there is no unauthorised use of the Association's time e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications;
- to ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked;
- to ensure that all employees are treated with respect, by discovering and eliminating any material that is capable of amounting to unlawful harassment.

Communications of a sensitive or confidential nature should not be sent by e-mail because it is not guaranteed to be private. When monitoring e mail, the Association will, save in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the Association may open e-mails and access the content. In this case, the Association will avoid, if possible opening e-mails clearly marked as private or personal.

The Association reserves the right to deny or remove e-mail or Internet access to and from any employee.

Sanctions for breaches

Employees who are discovered contravening the rules of this policy may face serious disciplinary action under the Association's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

Student contravention will be dealt with by Discovery College Cause for Concern (CFC) procedures.

Vandalism of, or otherwise intentionally interfering with, the Association's computers/network constitutes a gross misconduct and could render the employee liable to summary dismissal under the Association's disciplinary procedure.

Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of the Association's time, offensive material sent by e-mail is capable of amounting to unlawful harassment.

Employees who are discovered unreasonably using the Association's computers for personal and private purposes will be dealt with under the Association's disciplinary procedure.

Telephony including mobile phones

Land lines are provided for business use and it's essential that costs are kept to a minimum. Some local personal calls are permitted if kept to a minimum and of short duration.

No personal long distance calls are allowed.

YMCA Plymouth recognises mobile phones as an effective form of communication, we accept they are now part of everyday life.

At the same time, mobile phones are a distraction in the workplace. This policy covers mobile phones calls, texting and picture messaging.

We allow mobile phones only to be switched on during breaks or lunch times. On some occasions an employee may request that they are allowed their mobile phone switched on at work for a specific reason. Each request will be considered and judged on its own merits.

Mobile phones and driving

The use of a hand held mobile phone when driving is illegal. The use of mobile phones (hands free) whilst driving is actively discouraged and voice mail used instead. The use of hand-held mobile phones is not permissible in any circumstances.

Breach of the mobile phone policy may result in disciplinary action.