

# 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, email, 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.

### **Device security**

Those individuals who are required to use the Association's devices (PCs, Laptops, Tablets etc.) to carry out the duties of their role will be issued with a device and account login. These individuals are entitled to use these devices for work purposes only - not personal use apart from the limited exceptions detailed 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 visibly left out overnight in an office or other location. It should always be stored away safely, wherever possible in a lockable drawer or cabinet.

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

Discovery College students have their own guidelines for correct care of student devices which will be outlined in the student induction. This includes all devices being logged and returned securely to their storage cabinet at the end of the lesson.

## **Cyber Security**

Authorisation for access to the Association network is based on the requirements of the individual's job as stipulated in their job description. 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 and must follow [secure password guidelines](#). 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 account and device and must ensure that it is not used by an unauthorised person. To ensure this is not possible users must ensure that their device is 'locked' when they are away from the device for any period of time.

Staff users must also enable 2-Step Verification (2FA) for their work Google Account.

When using any non-YMCA owned device (i.e. a personal laptop or phone) which is then used to access or store work data (including using email, work-related documents etc.) employees must adhere to the same password standards as above. Additionally, it is the employees responsibility to ensure that antivirus software is installed on these personal devices. The Association recommends using trusted free anti-virus software that is compatible with all devices (iPhone, Windows, Android etc.) such as Avast, Norton, AVG and Bitdefender. The employee is welcome to purchase premium subscriptions of any antivirus software if they wish at their own expense.

## **Discovery College Webfiltering & Online Safety**

Relating to our safeguarding policy we have in place active web filtering in place across our network and devices used by Discovery College students. This includes active web filtering which blocks access to potentially unsafe and inappropriate material. The system is certified in accordance with KCSI guidelines and has Google SafeSearch features enabled.

## **External media**

You must not attach any external media (USB stick, SD card, HDD etc.) to transfer data without prior approval. This is to prevent the possible introduction of viruses.

### **Personal Usage of a Device**

Any personal usage of any device (i.e for internet browsing, video streaming, gaming, shopping, social media etc.) is not permitted within working hours. On a YMCA-owned device, personal usage is additionally not permitted even outside of working hours, except for the limited period of time in a set break during your working day (such as at lunch). Limited exceptions to this may only be made with permission from your line manager if the usage is deemed necessary and reasonable.

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). Web filtering for Discovery College is in place to prohibit access to any potential inappropriate websites as outlined above.

### **Storage and Data Protection**

All storage of work-related data on YMCA or non-YMCA devices must be in compliance with our Data Protection policy and Data Protection law. No non-work related personal data such as photographs, music, videos etc. should be stored on your YMCA account cloud storage or the local device storage. Our Bring Your Own Device to Work policy outlines how to handle security and data when using your own personal non-YMCA device for work purposes.

### **Downloading, sharing and messaging**

Downloading, sharing and/or using messaging apps to circulate 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. This extends to private staff group chats on messaging apps such as WhatsApp or closed social media groups.

When downloading 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 licence 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 Media**

Whether employees use social media 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 has the potential to damage the reputation of YMCA Plymouth, 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 media 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 social media and/or messaging apps 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 media 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.

Where social media is used for work purposes (ie. marketing and promotion, communications with clients etc.) relevant approval must be sought from a line manager where appropriate and professional standards must be maintained in all communications.

Social media policy for student is outlined within the student induction and is only allowed with explicit permission from a tutor.

## **Email**

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

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

Users are not permitted to use email for personal and private purposes during their normal working hours and are not permitted to use their YMCA email account for any personal purposes, including signing up to websites and accounts.

The forwarding and sending of offensive email 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 email addresses should report as spam, delete and not respond to such emails. Alternatively, if a user receives this type of email from an internal email address they should

forward the email to Human Resources Business Partner for action to be considered against the sender, under the disciplinary policy and then delete the email from their system.

Users are prohibited from using email to circulate any non-work related material including external promotions except with consent from a line manager.

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

Only relevant emails 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 redirected 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 email access increases the risk of employees inadvertently forming contracts through email and increases the opportunity for wrongful disclosure of confidential information. In addition, carelessly worded email can expose the Association to libel. As such, email 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 emails 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 email to send or receive 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 email because it is not guaranteed to be private. When monitoring email, the Association will, save in exceptional circumstances, confine itself to looking at the address and heading of the emails. However, where circumstances warrant it, the Association may open emails and access the content.

The Association reserves the right to deny or remove email 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 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 email is capable of amounting to unlawful harassment.

Employees who are discovered unreasonably using the Association's devices 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.

Mobile phones can be a distraction in the workplace and should not be used for non-work purposes during working hours unless explicitly necessary (i.e For a family emergency or to take a callback from a doctor). This policy covers mobile phone calls, instant messaging and other forms of communication on a phone.

### **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.