Title:	**E-safety and Acceptable Use of Technology Policy**
Reviewed by:	Judy Lye-Forster Designated Child Protection and Safeguarding Lead March 2017
Approved by:	Yeovil Youth Theatre Committee April 2017
Date of next review:	April 2019
Associated documents/policies:	**YYT documents/policies:** Child Protection Policy Equality Policy Members Code of Conduct Staff & Volunteers Code of Conduct **External documents/legislation:** Working Together to Safeguard Children 2017 Keeping Children Safe in Education 2016 Safeguarding Vulnerable Groups Act 2006 Ofsted publication 'The safe use of new technologies' 2010 The report of the Byron Review 'Safer children in a digital world' 2008 Guidance accessed from the following websites – www.swgfl.org.uk www.nextgenerationlearning.org.uk www.rsc-south-west.ac.uk www.ceop.gov.uk www.thinkuknow.co.uk

Contents

1 Objectives

To outline Yeovil Youth Theatre's approach to e-safety, as part of our commitment to safeguarding and to inform staff, volunteers and members of the company's policy on the acceptable use of technology.

2 Background/Scope

The company actively encourages members, staff and volunteers to fully exploit the power of technology. The company is keen to ensure all members enjoy accessing technology and use it safely as part of their learning. To support this aim, the company will take the approach of a managed system, rather than a 'locked down' approach. The company will provide information, support and guidance for e-safety which enables staff, volunteers and members to acquire the skills necessary to become independent, confident, safe and responsible users of technology. This information will include what to do in the event of an unwanted or unsafe incident.

The company, to such extent as is reasonable, has a responsibility to regulate the behaviour of staff, volunteers and members when they are outside of company activity and will impose disciplinary penalties for inappropriate or gross misconduct behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of company activity, but is linked to their role or membership of the company.

3 Appendices

Appendix 1 – Acceptable use of technology
Appendix 2 – E-safety policy for members
Appendix 3 – Social networking guidance for staff and volunteers (e.g. Facebook and Twitter)

4 Procedure

The growth of the internet and the development of mobile technology have created an exciting and stimulating world with great opportunities for exploration, learning and social interaction. It should be acknowledged however, that the use of these technologies can put people at risk, within and outside of the company's activities. For example:

- Access to illegal, harmful or inappropriate images
- Possessing, accessing or uploading any extremist materials, or using extremist language or expressing extremist views that could cause harm or distress
- Sharing personal contact details and information
- The risk of being subject to grooming by those with whom contact is made on the internet or social media sites
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers

- Cyber-bullying
- Access to unsuitable video / internet games
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and well-being of a young person or vulnerable adult.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, to assist members, volunteers and staff in acquiring the skills to remain safe whilst accessing technology and not to deliberately or inadvertently expose their peers to such risks.

4.1 E-safety policy for members

Members will be made aware of the e-safety policy through various methods as part of their introduction to the company. By signing the members code of conduct form they are already agreeing to comply with all company policies. Members and parents will be reminded of their responsibilities periodically via the company website and official company communications.

4.2 Social Media policy for staff and volunteers

- Company related social media sites or logins should be registered using the creator's company email address
- All sites must be added to the Company's Social Media Site Register. Where possible the IT Manager must be made an administrator of the site or group
- Advice on how to do this can be sought from the IT Manager
- Consent from members should be sought before any member details are added to a social media site
- Staff and volunteers should not use personal social networking sites to send or receive personal, non-work or work related messages with members
- Advice on e-safety should be made available on or from the website
- Active social media sites should be supervised by the creator and the IT Manager should be informed when they are closed or removed
- The creator of company social media sites must ensure that all equality & diversity, safeguarding and e-safety policies are adhered to
- Any instances of abuse experienced by staff, volunteers or members on social media sites should be reported to the Designated Safeguarding Lead immediately.

4.3 Dealing with incidents

safeguarding@yeovilyouththeatre.org.uk

This e-mail can be used in the event of an e-safety incident, but members are primarily encouraged to report any incident to any staff member or volunteer in the vicinity immediately.

Staff and volunteers should contact the designated safeguarding lead. If appropriate, the company's disciplinary procedures will be invoked. The safeguarding lead should be informed if anyone's safety or well-being is

considered to be at risk. It may be necessary for them to inform the police and/or the local safeguarding children board.

4.4 Use of digital and video images - Photographic, Video

- The development of digital imaging technologies has created significant benefits to learning, allowing staff, volunteers and members instant use of images that they have recorded themselves or downloaded from the internet, for the purposes of refining their performance. However, staff, volunteers and members need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees
- When using digital images, staff and volunteers should inform and educate members about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff and volunteers are permitted to take digital / video images to support educational aims within rehearsals and performance, but must follow company policies concerning the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images that members are appropriately dressed and are not participating in activities that might bring the individuals or the company into disrepute
- Staff, volunteers and/or members must not take, use, share, publish or distribute images of others without their permission
- Photographs published anywhere that include members will be selected carefully and will comply with good practice guidance on the use of such images
- Digital/ video images taken during rehearsals for the sole purpose of progressing the members performance will only be uploaded to the closed company YouTube channel and must not be further distributed outside of this platform
- Only those members of the company, staff and volunteers who have genuine reason to view these will be sent links to access the footage, these links must not be forwarded to third parties without the express permission of the original sender
- Written permission from parents or carers will be obtained before photographs of members under 18 years old are published on the company website or any other promotional material.

4.5 Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4.6 Communication

When using communication technologies the company considers the following as good practice:

- All members of staff and volunteers will be designated an official Yeovil Youth Theatre e-mail address on appointment to the company
- The official company email service may be regarded as safe and secure and is monitored. Staff and volunteers should therefore use only the company email to communicate with others when on company business.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the company policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff, volunteers and members or parents / carers (email, chat, texting, social networking etc) must be professional in tone and content. Personal e-mail addresses must not be used by staff and volunteers for these communications
- Personal information should not be posted on the company website and only official email addresses should be used to identify staff and volunteers
- All communication with company members should also be copied to parents/carers and sent via group e-mail as well as being posted on the website members area and as appropriate on the YYT Facebook page
- All communication with committee members with regard committee business should be sent via official YYT e-mail addresses only
- Breach of this guidance may result in disciplinary action.

4.7 Training

It is essential that all staff and volunteers understand their responsibilities.

- The Committee must ensure that all staff and volunteers fully understand the company e-safety policy and acceptable use of technology policy
- Training, where necessary, will be provided to new members of staff and volunteers
- The IT Manager will additionally provide advice / guidance / training as required to individuals
- Parents/carers should be provided with information about the company's e-safety policy and how to help keep young people and vulnerable adults safe when using ICT at home.

4.8 Safety and security of company website and social media sites

- All users will have clearly defined access rights to the company website and social media sites
- All users will be provided with a username and password, by the IT Manager, who will keep an up to date record of users and their usernames
- Users will be required to periodically change their password. Passwords will be reset at the beginning of each membership year
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and

must immediately report any suspicion or evidence that there has been a breach of security

4.9 Roles and Responsibilities

- **The Committee** are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. They are additionally responsible for ensuring the safety (including e-safety) of members of the company community, though the day to day responsibility for e-safety will be delegated to the IT Manager and the designated safeguarding lead.

- **All Committee members** should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or volunteer.

- **The IT Manager and the designated safeguarding lead jointly**
  - act as the e-safety co-ordinators
  - report on e-safety to the committee
  - take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the company e-safety policies / documents
  - should be trained in e-safety issues and be aware of the potential for serious child protection issues
  - provide training and advice for staff and volunteers and information for parents
  - ensure that all staff and volunteers are aware of the procedures that need to be followed in the event of an e-safety incident taking place
  - liaises with the Local Safeguarding Children Board and Police
  - receive reports on e-safety incidents and create a log of incidents to inform future e-safety developments

- **The IT Manager** is responsible for ensuring that the company's website and social media sites are secure, are not open to misuse or malicious attack and meet the e-safety technical requirements of the company's e-safety policy.

- **All Staff and volunteers are responsible for ensuring that they:**
  - have an up to date awareness of e-safety matters and of the current company e-safety policy and practices
  - have read, understood and agreed to comply with the company E-Safety and Acceptable Use of Technology Policy
  - report any suspected misuse or problem
  - embed e-safety awareness in their delivery of teaching and learning

Appendix 1 - Acceptable Use of Technology

Introduction

The company actively encourages members, volunteers and staff to fully exploit the power of technology to help with teaching and learning. The company is keen to ensure all members enjoy accessing technology as part of their learning and can do so safely. This document sets out what the company considers to be an acceptable use of technology and also makes clear what behaviours are not acceptable.

What you <u>can</u> do...

- Use the company website and social media sites for company related business
- Use the company e-mail addresses of staff and volunteers to communicate with them about company related business

What you can do to help others...

- Assist other members in using technology safely
- Bring to the attention of staff and volunteers any instances of bullying or harassment via the company sites or e-mail addresses

What you <u>must</u> do...

- Take responsibility for your own use of technology making sure you use it safely and legally
- Respect the rights of others when accessing technology
- Keep your company login details secure
- Respect all copyright notices when accessing the website
- Report to a member of staff any failings in the technical safeguards you are made aware of.

What you <u>cannot</u> do...

- Possess, access or upload any extremist materials
- Access any system in a way that brings the company into disrepute
- Deliberately evade any technical systems that are provided by the company to safeguard users
- Exploit any system (company or privately owned) in a way that caused distress to another company member or member of staff or volunteer
- Attempt to access, change copy or destroy other users' work.

What you should be aware of...

- All users should be aware that activity and online communications made via the company systems may be monitored. This is done to reassure all users that they are working in safe, legal environment free from inappropriate, threatening, extremist or illegal activities
- Users who are found to have broken this policy will be subjected to the company disciplinary procedure.

Appendix 2 - E-safety and Acceptable Use of Technology Policy for Members

Members must use the company systems in a responsible way, to ensure that there is no risk to personal safety or to the safety and security of the systems and other users.

1. **For your own personal safety:**
   - understand that the company will monitor your use of the systems, social media, email and other digital communications
   - treat your username and password as confidential – do not share it, nor try to use any other person's username and password
   - protect yourself from unwanted or potentially dangerous contact from people unknown to you when you are communicating on-line
   - do not disclose or share personal information about yourself or others when on-line
   - immediately report any unpleasant, inappropriate or extremist material or messages or anything that makes you feel uncomfortable when you see it on-line.

2. **Understand that everyone has equal rights to use technology as a resource and:**
   - understand that the company systems are primarily intended for educational use and that you will not use the systems for personal or recreational use unless you have permission to do so.

3. **Act as you expect others to act toward you:**
   - respect others' work and property and do not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
   - be polite and responsible when you communicate with others, do not use strong, aggressive or inappropriate language and appreciate that others may have different opinions
   - do not take or distribute images of anyone without their permission
   - only use chat and social networking sites with permission and at the times that are allowed.

4. **Understand that you are responsible for your actions, both in and outside of company activities:**
   - understand that the company also has the right to take action against you if you are involved in incidents of inappropriate or gross misconduct behaviour, that are covered in this agreement, when you are outside of company activity and where they involve your membership of the company community (examples would be cyber-bullying, use of images or personal information)
   - understand that if you fail to comply with the E-Safety and Acceptable Use of Technology Policy, you will be subject to disciplinary action. This may include loss of access to the company members site on the website, suspensions or permanent exclusion from the company, contact with parents and/or partner educational institutions and, in the event of illegal activities, involvement of the police.

Appendix 3 - Social Network Guidance for Staff and Volunteers

Introduction

Social media provides excellent opportunities for teaching and learning as well as opportunities for staff, volunteers and members to communicate and engage with each other and subjects of interest. The company appreciates the power of social media to enrich their personal, academic, artistic and professional lives and therefore aims to encourage the safe and productive use of social media.

Online conduct

- The company's policy on Equality and the Code of Conduct apply whether staff, volunteers and members are in rehearsal or online on company business
- Staff, volunteers and members should not make comments that could be considered to be bullying, harassing, discriminatory or extremist against any individual
- Staff, volunteers and members should not post offensive or derogatory comments
- Language and forms of address should be appropriate for a professional setting
- Staff, volunteers and members should not post anything that could bring the company into disrepute or damage the company brand
- Staff and volunteers must ensure that they adhere to the same standards of confidentiality online as they would in rehearsal.

Online safety

- The company has clearly defined responsibilities towards children and vulnerable adults. Anything disclosed to a staff member or volunteer on social networking sites should be treated in exactly the same way as if it was face to face and must be reported to the designated safeguarding lead
- Should staff, volunteers or members have any fears or concerns while using social networks and media, e.g. victim of cyber bullying, a cyber theft, inappropriate communications or exposure to extremist material etc. they should immediately contact the designated safeguarding lead or email *safeguarding@yeovilyouththeatre.org.uk* with details
- It is recommended that staff and volunteers keep their personal and professional lives separate online by using their company email account to create a separate online presence and conducting themselves in a professional manner
- Staff, volunteers and members should take care when divulging personal details, age, address, family information. For example, Facebook provide 'privacy settings' (accessed via the Account link) to enable users to control what information is accessible to the wider Facebook community and the Internet. Staff and volunteers are strongly advised to review and understand how these settings work. If you are not certain it is recommended that you select the 'friends only' option
- There are no privacy settings in Twitter. It is essential that staff and volunteers maintain a professional stance when posting on this social network. Everything posted is available to everyone. Staff should refrain from commenting on other tweets in a manner which appears to represent the company's viewpoint. Personal posts and status updates should be on personal accounts only

- The IT Manager should only accept current members on the YYT Facebook site and should not arrange to meet members using Facebook unless it is at company rehearsal during normal rehearsal hours for the purposes of company business
- The IT Manager should only accept current and former members on the YYT Alumni Facebook site and should not arrange to meet members using Facebook unless it is at company rehearsal during normal rehearsal hours for the purposes of company business
- Staff, volunteers and members should never arrange to meet anyone alone that they have been introduced to online. Any such meetings should be risk assessed and notified to the committee
- Care should be exercised in the use of photographs and other visual media. Permission should be sought before posting images of staff, volunteers and members in line with existing company policy
- Anything, even slightly suspicious, should immediately be reported to the designated safeguarding lead so that it is logged
- Ensure that members understand the benefits and risks of using Social Media
- Staff, volunteers and members should seek advice and/or training before using social media for company projects
- Some software and media available on social sites is harmful. Only download files essential to company work and regularly run the virus checker on your computer, tablet, mobile device or USB stick/flash drive. Beware of commercial apps and quizzes circulated on social networks that are not produced by a preferred provider.

In particular staff should be aware that

- copyright and data protection laws apply online. The JISC Legal Information website provides some information on these issues. If in doubt, consult their website before proceeding
- not all staff, volunteers and members will have access to, or want to access social networking sites. In these cases personal preferences and concerns should be respected. Alternatives should be provided where needed
- the needs of staff, volunteers and members with a disability should be considered when requiring the use of any online system.

Additional Information

The UK's first ever helpline for professionals, specifically dealing with e-safety issues has been launched. The helpline is part of the UK Safer Internet Centre (www.saferinternet.org.uk) and is for all professionals and volunteers who work with children and young people, and aims to address online safety issues they face, both professionally and personally.

The helpline, based in Exeter, is available by email via helpline@saferinternet.org.uk or from 10am to 4pm (Mon to Fri) on 0844 381 4772.