Hampshire Futures

Inspiring ambition, supporting success

Adult & Community Learning, Pre-apprenticeship and Apprenticeship

Internet and e-safety

Policy and Procedures

Date of last review/update:
December 2018

@hantsfutures @hantsfutures

Hampshire County Council

www.hants.gov.uk

Contents Page

Internet & e-safety

'the contents of this policy is an integral part of the HF Quality Improvement Framework'

1. Purpose

Hampshire Futures aims to provide a safe and secure learning environment for all staff and learners.

Hampshire Futures is committed to ensuring a consistent approach is adopted in respect of internet and e-safety for all staff and learners across its ESFA funded programmes (Study Programmes; Traineeships; Apprenticeships; and Adult and Community Learning (ACL)) regardless if these are delivered directly by Hampshire Futures or one of its sub-contracted partners.

2. Scope

The primary duty of care in respect of the safety of staff and learners whilst using the Internet and e-technologies is the responsibility of; Hampshire Futures through its direct delivery team on all study programmes, traineeships and apprenticeship programmes; and of the Learning Provider contracted through a funding agreement with Hampshire Futures to deliver adult and community learning.

Hampshire Futures will work in partnership with all relevant stakeholders and learning providers to promote and secure the concept of the "safe learner" in respect of internet and e-safety safety.

3. Implementation

Hampshire Futures will ensure that the safety of staff and learners whilst using the Internet will be facilitated by the relevant learning providers

All learning providers will take such precaution as is reasonably practical to provide and maintain safe and healthy working/learning conditions for staff and learners.

The use of the Internet, email and other e-technologies by staff and learners is permitted and encouraged where such use supports the goals and objectives of the learning programme.

All learning providers will have their own internet safety policy, and this should include practical steps that will achieve the objectives of this policy by providing and maintaining high standards of safety for staff and learners, as far as is reasonably practicable.

The inclusion of an internet safety element in all relevant Hampshire Futures contract documents, places the primary duty of care with the learning provider.

The provider will:

- do everything possible to ensure that hardware, software and networks are safe and secure, for example using filtering, encryption, firewalls and anti-virus software

- assess their use of technology for risks to staff, learners and information security. The assessment should be recorded and include any actions taken to mitigate any risks, including the risk of learners accessing websites linked to radicalisation and extremism
- ensure that all users of technology abide by the Councils and/or their learning providers Acceptable Use Policy/Statement - see Appendix 1
- provide support to staff and learners where necessary to ensure that they understand their responsibilities according to the Councils and/or their learning providers Acceptable Use Policy/Statement
- deal with any breach of the acceptable use statement or policy in a timely manner, including, if necessary, referring to the Safeguarding and Prevent policy, or reporting to the police in the case of illegal activity.

Communications

We recognise that the use of e-technologies for communication can greatly enhance the learning experience. Therefore, Providers should:

- consider carefully which modes of communication will be useful to them
- give guidance to learners to ensure that they know how to use communication technology, including social media, in a way which is safe and prevents radicalisation and extremism.

Use of recordings – audio/images/video

The use of recordings can be very beneficial to learning, teaching and assessment and the associated risks should be carefully managed. Providers will:

- ensure that permission is sought to use recordings of learners and staff/volunteers
- carefully assess the use of recordings of any type when sharing or distributing online to ensure that the use does not place any individual in a vulnerable position, or go beyond permissions granted by individuals.

Social media

When thinking about using social networking, a common sense approach should be taken. Safeguarding principles and basic manners in how we communicate with people must be adhered to. If it is right and proper to be courteous, discrete and professional when communicating with people in person (inside or outside of the organisation) then the same rules should apply when typing anything into a computer or a communication device. Likewise if the rules to keep young people and adults safe and the sharing of information protocols within the organisation are important when dealing face to face with people, the same principles should again apply when posting anything onto the World Wide Web.

Social networking websites and applications include, but are not limited to:

- Snapchat (photo & video)
- Facebook (text, photos, videos, and personal profiles)
- You Tube (videos, user comments, and personal profiles)
- Instagram (photos and videos)
- Twitter (text and photos)
- Webinars (a seminar conducted over the Internet)

All these sites allow individuals and groups to communicate using a variety of communication methods. Learners will be able to use social media sites/apps within a learning environment in accordance with their tutor's instruction, as long as it is part of their course.

Befriending: One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. Staff should maintain a boundary between their professional and personal lives and should not to accept personal invitations to "friend" learners (children or young people) or initiate personal friendships with learners, or learners' family members/friends.

Security: Learners and staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly. Even with privacy settings in place it is still possible that the personal details of learners and staff may be accessed more broadly than the other networkers identified by them. In using social networking sites, learners and staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible.

Training for staff

Hampshire Futures and its sub-contracted providers will ensure that staff and volunteers receive information and training, as appropriate, to ensure that they:

- Understand internet and e-safety issues and risks
- Abide by the Councils and/or their learning providers Acceptable Use Policy/Statement
- Are aware of where to go to get help and advice
- Are aware of the reporting the appropriate reporting procedures
- Embed e-safety, as appropriate, in their teaching practice
- Can access relevant e-learning resources on e-safety and the Prevent Duty from for example https://www.getsafeonline.org/ and the Education and Training Foundation.

Reporting Procedure

Hampshire Futures and its sub-contracted providers will:

- advise learners to report any e-safety incident, including those related to radicalisation and extremism to their tutor or other members of the provider staff.
- advise staff to report any e-safety incident, including those related to radicalisation and extremism to their line manager.
- advise staff if they become aware that a learner (or group of learners) has made inappropriate/insulting/threatening comments about another learner or a member of staff on a social networking site; they must report this to their line manager so that the appropriate action can be taken.
- record any incidents and the course of action taken to remedy the situation.

Where the misuse presents a safeguarding concern, Hampshire Futures Designated Safeguarding Officer will intervene.

Appendix 1 (also included in the Hampshire Futures learner handbooks)

Acceptable Use Statement

Use of the Internet and email by learners is permitted and encouraged where such use supports the goals and objectives of the learning programme.

Hampshire Futures has a policy for the use of the Internet and email whereby learners must ensure that they:

- follow any given guidelines to stay safe online
- comply with current legislation
- use internet and email in an acceptable way
- do not create unnecessary business risk to Hampshire Futures, or to their learning provider, by their misuse of the internet/email.

Unacceptable behaviour

The following behaviour by a learner is considered unacceptable:

- use of Hampshire Futures or Providers communications systems to set up personal businesses or send chain letters
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- transmitting unsolicited commercial or advertising material
- introducing any form of computer virus or malware into the corporate network

Appendix 2

Links with other policies/guidance

Hampshire Futures Safeguarding and Prevent Policy
Policy and Procedures - Safeguarding & Prevent Policy
Hampshire County Council's Photography and Video Consent Forms
Hampshire County Council Information governance and security policy and guidance
http://intranet.hants.gov.uk/information-security/information-security-policies.htm
http://intranet.hants.gov.uk/information-security.htm
http://intranet.hants.gov.uk/information-security/information-security-policies/infsec-acceptableuse.htm
Hampshire County Council's Social Media Policy, and Social Media Guidance

Link to useful websites
www.thinkyouknow.co.uk
www.digizen.org
www.childnet.com
www.ceop.gov.uk
www.facebook.com/safety
www.getsafeonline.org
www.chatdanger.com/mobiles