E-safety and Acceptable Use of ICT Policy

This E-safety and Acceptable Use of ICT Policy (AUP) relates to all members of the Alt Valley Community Trust (including learners/participants, staff, volunteers, visitors and contractors) who have access to, and are users of ICT systems and resources both in and out of venues where actions relate to AVCT set activities or use of AVCT online systems.

Context

To prepare learners/participants for the needs of today and their future working lives where the curriculum/activities and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and learners/participants into contact with a wide variety influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the AVCT environment. Current and emerging technologies in AVCT and more importantly, in many cases outside the AVCT by learners/participants include:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- PDA’s
- Smart phones with e-mail and web applications

All of these have potential to help raise standards of teaching and learning and delivery of activities, but may equally present challenges to both learners/participants and tutors/leaders in terms of keeping themselves safe. These challenges include:

- Exposure to inappropriate material
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identify theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising online gambling and financial scams
- Safeguarding issues such as grooming (Children or vulnerable adults)
- Radicalisation and Terrorism
- Other illegal activities

All Internet and email usage must comply with:

- The five fundamental British Values of democracy, rule of law, individual liberty, mutual respect and tolerance of different faiths and abilities
- The Prevent duty, the purpose of which is to reduce the threat to the UK from all forms of terrorism by stopping people being drawn into terrorism and/or extremism.

Learners/participants/should be aware that traffic and content may be monitored and appropriate action will be taken if necessary.

At Alt Valley Community Trust we seek to maximise the benefit that can be obtained by exploiting the use of ICT, whilst at the same time minimising any associated risks. By making clear to learners/participants, staff, volunteers, contractors etc. what the AVCT expectations are regarding the use of ICT, we aim to protect our learners/participants and staff from harm, as far as reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads and fashions change but there are general principals of behaviour and the code of conduct that apply to all situations e.g.: all users need to know what to do if they come across inappropriate material, and that staff members should not give out their personal information to learners/participants such as their personal telephone numbers, email address or allow access to their personal social networking site accounts etc. We must also communicate to young people and vulnerable groups on courses at Alt Valley that they should not give out their personal information such as telephone numbers; addresses etc to strangers or publish this information on social networking sites.

A balance needs to be struck between educating staff and learners/participants to take a reasonable approach towards the use of regulation and technical solutions. We must recognise that there are no totally effective solutions to moderate and control the Internet, so this policy incorporates both approaches.

Roles and Responsibilities

Staff

All teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout the AVCT and following e-safety procedures. All AVCT staff should be familiar with the E-safety and Acceptable use of ICT policy (AUP) as well as their relevance to the code of conduct and safeguarding policies.

- All staff should have read, understood and accepted the Staff Acceptable Use Agreement
- Act in accordance with the AUP and e-safety policy
- Staff should report any suspicion of misuse to the designated persons or line manager
- Staff should refrain from making negative comments about learners/participants within the AVCT environment. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the AVCT and/or lowers morale.
- Staff should help educate learners/participants in keeping safe especially with vulnerable groups. Whilst regulation and technical solutions (such as filtering systems) are important, they must be balanced with educating learners/participants to take a responsible approach. The education of learners/participants in e-safety is an essential part of using technology in classes. Staff should act as a good role model in their own use of ICT.
- Where Internet use is pre-planned in sessions or enrichment activities, learners/participants should be directed to sites which are appropriate for their use and procedures should be followed for reporting any unsuitable material that is found on Internet searches. Where practicable staff should pre-check sites and any possible searches.
- Where learners/participants are able to freely search the Internet staff should be vigilant in monitoring the content of websites in case there is any unsuitable material.
- Staff should be aware of the potential for cyber-bullying in their sessions where malicious messages through social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.
- Learners/participants should be taught to be critically aware of the materials/content they can access online and be guided to validate the accuracy of information.

- Learners/participants are educated to of the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the Internet.

Learners/participants

The provision of ICT resources and facilities are a privilege, not a right. Learners/participants are encouraged to access various technologies in sessions, private study and in the completion of assignments and independent research, and are therefore expected to follow the AVCTs AUP. They should fully participate fully in e-safety activities and report any suspected misuse to a member of staff. Learners/participants are required to sign an agreement to state that they agree to the terms of our AUC policy and their e-safety responsibilities:

Learners/participants are expected to:

- Behave in a safe and responsible manner
- Treat equipment with respect
- Use USB/flash memory key(s) only for AVCT purposes
- Be polite and not use e-mail, social media or blogs etc to make negative comments, bully or insult others
- Use the resources only for educational purposes

Learners/participants are expected not to:

- Waste resources including Internet and printers
- Eat or drink in the ICT Suites
- Use someone else's login details
- Have any inappropriate files (e.g. copyrighted or indecent material)
- Attempt to circumvent or "hack" any systems
- Use inappropriate or unacceptable language
- Reveal their personal details or passwords
- Visit websites that are offensive in any way
- Use chat rooms or newsgroups
- Do anything that could damage the reputation of the AVCT
- Download anything inappropriate or install any programs

Senior Management Team

The senior management team at Alt Valley Community Trust take e-safety very seriously and will ensure that policies and procedures are in line with best practice and the safeguarding

agenda. In particular, they will ensure that all staff receives suitable training and development to carry out their e-safety roles and sufficient resources are allocated to the task. Senior managers will follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff and ensure that there is a robust system in place for monitoring e-safety. This includes making sure that the Network infrastructure is safe and secure and those policies and procedures approved within this policy are implemented. Regular review of the issues will take place at the safeguarding working group meetings with feedback sessions scheduled to the senior management team meetings.

Responding to issues

It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the AVCT community are aware those incidents have been dealt with.

Any concerns around the misuse of ICT must follow the referral process within the Safeguarding Policy and Procedure where there is a potential threat to another learner, vulnerable person or member of staff. Any suspected misuse must be reported to a member of staff and then an appropriate course of action will be agreed.

Where it is suspected that any misuse might have taken place the relevant member of staff will depend on the nature of the misuse and AVCT disciplinary procedure will be invoked.

Where an allegation has been made against a learner/participant an investigation will take place by the designated persons of the safeguarding working group. The outcome of the investigation will decide what will be the appropriate course of action and depending on the nature of the misuse the learner/participant could be suspended from classes/activities until the investigation is complete. The student code of conduct procedure will be invoked should the allegation be found to be true and the sanction will depend on the seriousness of the misuse and whether it was accidental or deliberate, a first-time offence, thoughtless or malicious e.g. intended to cause harm to others. Sanctions could involve the learner/participant having ICT access removed for a period of time or in very serious cases, exclusion. Where there is a potential legal issue the Head of Education or Deputy Chief Executive will decide on the need for involvement of outside agencies including the police, together with the designated persons and Senior Management team in line with our Safeguarding and other policies.

AVCT Wi-Fi Network

AVCT provides a guest wireless network which is available to all teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff). Use of this provision is

governed by the AVCT's E-safety and Acceptable Use Policy and by logging onto the network the user is deemed to have agreed to abide by AVCT Acceptable Use Policy.

All users utilising the guest wireless connection should be aware of and agree to conditions of use including but not limited to the following:

- AVCT assumes no responsibility for the safety of equipment or device configurations, security, or data files resulting from connection to the AVCT's guest wireless network or the Internet, nor liability for any damages to hardware, software or data, howsoever caused.
- Guest wireless access is provided as a free service on an "as is" basis with no guarantee of service.
- Staff cannot assume any responsibility for personal hardware configurations, security or changes to data files resulting from connection to the guest wireless network. It is recommended that users make a backup copy of any settings before configuring their equipment for use on the guest wireless network.
- Use of the guest wireless internet connection is undertaken at the user's own risk. The wireless network protects users against basic malware/botnet/phishing protection; however, it is the responsibility of the user to protect their wireless devices through use of up-to-date virus protection, personal firewall and any other suitable measures.
- The guest wireless network may be subject to periodic maintenance and unforeseen downtime.
- Alt Valley Community Trust filters ALL Internet access.
- Printing access is not available via the guest wireless network. If the user desires to print, they will have to make their own suitable alternative arrangements.
- Any attempt to circumvent AVCT procedures or any unauthorised attempt to access or manipulate AVCT equipment or networks, may result in permanent disconnection from the guest wireless network and further disciplinary action being taken.