E-safety
and
Acceptable Use of ICT Policy
2020 - 2021

Produced by	Jeanette Martin
Approved by	Patricia Carlisle
Date Approved	July 2020
Review Date	June 2021

The London Borough of Merton is committed to providing high quality and sustainable adult learning in order to improve the social, economic, health and wellbeing of our residents. We deliver this through a strategic investment approach: commissioning provision to the best providers in the field and by developing sophisticated evidence based approaches to what we deliver.

This E-safety and Acceptable Use of ICT Policy relates to all learners attending courses through LBM (including with our providers, and the staff of those providers and partners) who have access to, and are users of ICT systems and resources both in and out of learning venues where actions relate to LBM adult learning activities.

Context

To prepare learners for the needs of today and their future working lives where the curriculum whether face to face or online, 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 learning, work, home, social and leisure activities is expanding across all sectors of society.

This brings learners and staff into contact with a wide variety of influences, some of which may be unsuitable and may pose safeguarding, radicalisation and/or extremism risks. Technology is enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the learning environment. Current and emerging technologies in learning and more importantly, in many cases outside the learning environment by learners include:

- Internet websites
- Communication platforms e.g. Zoom, Google Hangouts
- Virtual Learning Environments (VLE)
- Instant messaging
- Social networking sites
- Emails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones with email and web applications

All of these have potential to help raise standards of teaching and learning, but may equally present challenges to both learners and staff in terms of keeping themselves safe.

These challenges include:

- Exposure to inappropriate material including radicalisation or extremist websites and pornographic images
- 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)
- Other illegal activities

At LBM we seek to maximise the educational benefit that can be obtained by exploiting the use of ICT, whilst at the same time minimising any associated risks. By working internally and with our providers and partners to make clear to learners and staff what the expectations are regarding the safe use of ICT, we aim to protect our learners 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 principles of behaviour and conduct that apply to all situations e.g. all users need to know what to do if they come across inappropriate material, or someone accessing information that could be linked to radicalisation and/or extremism. It's essential that tutors are aware that their personal information must not be given out to learners such as their personal telephone numbers, email address or allow access to their personal social networking site accounts and so on.

A balance needs to be struck between educating staff and learners 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.

Responsibilities

All teaching and non-teaching staff (including partners, volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout the learning venue and following e-safety procedures. Providers should have an E-safety and Acceptable Use of ICT Policy in place and staff must be aware of the content of the policy and how it links to safeguarding.

We will (in partnership with our providers) ensure:

- staff behave in a safe and responsible manner, act as role models in the use of ICT and have access to e-safety training and awareness, and the E-safety policy.

- staff educate our learners in keeping safe on-line and when using ICT.

- staff and learners follow stringent codes of conduct when using online communication platforms for learning

- encourage learners to take a responsible approach when using or engaging with ICT.

- there is a process in place for reporting and investigation of any suspicion of misuse to a designated person or line manager and that the process includes the consequences of breaches of the policy and ICT misuse.

- we develop strong and supportive links with partners that will come into contact with our learners, to ensure there is a stringent information sharing protocol, training and reporting process.

- staff and learners refrain from making negative comments about learners, London Borough of Merton and/or the provider on any blogs or social networking sites.

- staff and learners refrain from using inappropriate or unacceptable language when using ICT.

- staff and learners do not share passwords or use someone else's log-in details

- staff pre-check sites and searches where internet use is pre-planned for sessions or enrichment activities. Learners 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.

- staff and partners are vigilant in monitoring the content of websites in case there is any unsuitable material where learners are able to freely search the internet such as in learner 'open access' areas.

- staff are aware of and inform learners of the potential for cyber-bullying or malicious messages e.g. through the use of forums and social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.

- Educate learners to respect the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the Internet.

Merton Adult Learning will monitor the safe use of ICT by our providers as part of quality assurance.

Learners
Learners are encouraged to access various technologies in sessions and when undertaking independent research, and are therefore expected to accept and follow the guidelines set out in the e-safety and acceptable use of ICT policy. They should participate fully in e-safety activities and report any suspected misuse to a member of staff.

Learners must:
- behave in a safe, appropriate, and responsible manner
- treat equipment with respect
- be polite and not use email to bully or insult others
- use the resources only for educational purposes

Learners must not:
- waste resources
- eat or drink when using LBM or provider ICT equipment
- 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
- download anything inappropriate or install any programmes

Reporting and investigation

Providers - Reports of suspicion or misuse for any person linked to a course being run by a provider on behalf of LBM should be made directly to the providers designated officer. Information on how this can be done will be available from the provider.

Partners- Will report suspicion or misuse for any person linked to a LBM course being run by a provider, to the Merton Adult Learning team by emailing a member of the team.

Serious breaches must be dealt with immediately, and full investigations must be completed within 10 working days of receipt of the information being received and actions set to ensure the issue does not happen again.

Serious breaches of e-safety or safe use of ICT may result in an amendment to contract terms for commissioned provision.

Related Policies, Procedures and Documents

- Safeguarding Policy
- The Counter Terrorism and Security Act 2015
- Prevent Strategy 2014-15
- Prevent Risk Assessment/Action Plan

This policy will be reviewed annually, or before should there be a significant change in guidance or policy.