SUPPORTED BY
MAYOR OF LONDON

Merton Adult Learning | merton

Digital and Acceptable Use of ICT Policy 2023 - 2024

Produced by	Jeanette Martin
Approved by	Patricia Carlisle
Date Approved	June 2023
Review Date	June 2024

The London Borough of Merton is committed to providing high quality and sustainable adult learning to improve the social, economic, health and wellbeing outcomes of our residents. We will 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 Digital and Acceptable Use of ICT Policy relates to Merton Adult Learning (MAL) staff, all subcontracted providers and their staff, all learners attending MAL courses, 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 MAL activities.

Our strategy includes that we will 'Embrace technological developments and support residents through the delivery of courses that improve learners economic and digital opportunities'.

We recognise that adults can experience isolation because of digital exclusion, this was particularly highlighted during the Covid-19 pandemic where life changed greatly. To help tackle isolation and exclusion, MAL will look to subcontracted providers to:

- deliver a range of digital skills courses
- include blended and remote delivery where appropriate
- use digital methods of teaching
- provide online resources and show learners how to access these safely

MAL providers that secured additional funding from the Greater London Authority (GLA) to purchase digital equipment, put this to good use and enable more learners to take part.

Context

To prepare learners for the digital needs of today through a curriculum that supports them to learn how to safely locate, retrieve and exchange information using a variety of technologies. Digital skills are vital to access employment, connect and interact socially, and as part of everyday life.

Digital use for learning, work, home, social and leisure activities is expanding across all sectors of society, and whilst there are huge benefits to this, we are mindful of the risks to vulnerable groups and the need to include how to stay safe online in our programmes.

The Covid-19 pandemic raised the need for a wider knowledge of digital skills and highlighted where there were gaps in learning and how MAL could bridge those gaps. MAL providers continue to utilise the additional digital skills developed during this time, to better support learners in their access to learning and develop their digital skills.

This policy was updated using information gained during the stages of our move to online delivery during the pandemic, and resources from a range of Adult Learning providers who found themselves going through the same process.

Digital usage 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:

- Smart phones
- Internet websites
- Platforms e.g. Zoom, Teams, Google Hangouts, Tik Tok, Facebook, Twitter, Instagram and YouTube. Also, some non-mainstream such as Parler or BitChute
- Virtual Learning Environments (VLE)
- Instant messaging, Social networking sites, and Chat rooms
- Emails
- Blogs, Podcasting, or Video broadcasting sites
- Gaming and gambling sites
- Music download sites
- Digital cameras

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, pornographic or intimate images, and hate speech
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identify theft, financial or personal scams, or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising or online gambling
- Safeguarding issues such as grooming (children or vulnerable adults)
- Other illegal activities

At MAL we seek to maximise the educational benefit that can be obtained by exploiting the use of digital technology, whilst at the same time minimising any associated risks. By working with our providers and partners to make clear to learners and staff what the expectations are regarding safe use, we aim to protect our learners 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 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 or offensive material, or someone accessing information that could be linked to radicalisation and/or extremism.

MAL will help providers to understand where behaviours in the use of online platforms move from being safe to concerning or worrisome. This includes, but is not limited to, identifying behaviours in the table below:

Insignificant behaviour	Troubling behaviour	Worrisome behaviour
Viewing and engaging with non-extreme content by accessing mainstream sites. Mentioning non-mainstream sites.	Accessing non-mainstream sites and specifically viewing concerning content. Mentioning seeing a concerning post.	Sharing or posting extreme content on any site. Agreeing with posts inciting violence, glorifying terrorism or dehumanising groups.

	Engaging with extreme content on non-mainstream sites. Viewing and accessing extremist content on mainstream sites.	Encouraging others to access extremist material online.

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 or online activity, so this policy incorporates both approaches.

CPD

MAL requires subcontracted providers to have a robust staff development programme in place that includes digital skills and the continued enhancement of the safe delivery of all learning including blended and online. Provider staff should be adept at utilising digital platforms and resources to ensure learners can participate in high quality learning. Tutors are required to create an environment that allows the learner to focus on learning, build their knowledge, and acquire skills to improve on what they already know and can do. Provider managers are required to identify development needs, act on those needs, and have ongoing monitoring processes in place.

MAL will request information on provider CPD plans as part of the quality assurance process and will monitor the impact during quality reviews and observations of teaching and learning.

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:

- Provider policies are communicated to ensure staff and learners are aware of the processes and procedures in place to stay safe whilst taking part in their learning.
- Staff have access to and complete online safety and awareness training.
- Staff keep their knowledge up to date and recognise emerging new technologies and platforms.
- Staff behave in a safe and responsible manner, act as role models in the use of ICT.
- Staff encourage learners to take a responsible approach when using ICT and teach them how to keep safe online and when using ICT.
- Learners are in an environment where they feel they can raise concerns.
- Staff and learners follow stringent codes of conduct that cover all methods of learning delivery including blended and online.

- Providers have effective firewalls and protection in place to give immediate alerts if a user types in anything (search engines or documents) that means they might be at risk.
- Providers have a training and awareness process in place for Cyber Security and take swift action should a breach occur.
- Providers ensure software installed or downloaded are in accordance with the appropriate licensing and adhere to copyright law.
- 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 interact 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, Merton Council and/or the provider on any digital platform including 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 can freely search the internet such as in learner 'open access' areas.
- Staff are aware of and inform learners of the potential for cyber-bullying, grooming or malicious messages e.g. through the use of forums and social networking sites, or via emails or text messages, which can cause hurt or distress.
- Providers 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:

- use someone else's login details

- reveal their personal details or passwords
- have any inappropriate files (e.g. copyrighted or indecent material)
- attempt to circumvent or “hack” any systems
- use inappropriate or unacceptable language
- visit websites that are offensive in any way
- use chat rooms or newsgroups
- download anything inappropriate or install any programmes
- eat or drink when using MAL or provider ICT equipment
- waste resources

Equipment

MAL providers should review their resources and equipment and advise MAL where additional items are needed to deliver high quality provision to a range of learners. Where possible MAL will loan this equipment to the providers or, if additional funding is available, will agree that the provider can purchase directly and invoice MAL.

An Equipment Loan Agreement is in place where MAL has purchased equipment for use by a provider. The agreement will include the terms and conditions the provider agrees to in respect of managing and maintaining the equipment, safe usage, and protection of data.

Providers can use a range of Platforms to deliver the provision e.g. Microsoft Teams, Zoom, Google Drive, YouTube. All methods used must be conducted safely and follow the providers policy and procedures.

Delivery

Through collaboration with our providers and in line with local and government priorities, MAL will enhance and develop the curriculum using a range of digital platforms and resources to meet the needs of our learners.

All blended, online and remote learning will continue to follow the MAL quality framework, safeguarding, RARPA guidelines, and meet the requirements of the Ofsted Inspection Framework.

Providers are required to follow the responsibilities listed within this policy, and in addition ensure:

- where online lessons (including breakout sessions) are recorded, learners are made aware of this and how they will be used, and there must be a process in place to securely store the recordings.
- observations of teaching learning and assessment for online, blended and remote delivery follows their OTLA policy guidelines.
- staff are aware of and adhere to working from home protocols.

Safeguarding

MAL providers must ensure all provision including blended, online and remote follows their Safeguarding and Prevent policies in place.

Policies must include the risks imposed through use of digital technology, online and remote learning activity, and how our learners and staff can stay safe.

Learners must be made aware of safeguarding and Prevent processes and procedures at induction and during their course programmes, and have clear understanding of who they should contact if they have a concern and how to keep themselves safe.

Reporting and investigation

Providers - Reports of suspicion or misuse for any person linked to a course being run by a provider on behalf of MAL 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 MAL 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.

Data protection

MAL providers must have processes and procedures in place to ensure both staff and learner personal information is kept secure and meets the requirements of data protection and GDPR policies in place.

Learner details must not be kept on personal computers or desktops and should only be kept within the providers secure access area.

Related Policies, Procedures and Documents

- Safeguarding & Prevent Policy
- MAL Strategy
- Equipment Loan Agreement
- The Counter Terrorism and Security Act 2015, including Prevent Duty Guidance
- Prevent Risk Assessment/Action Plan

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