

Data Protection Policy

(including GDPR)

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.

The Service operates through a commissioned learning service through providers at a number of venues. At each of these locations we work in partnership with representatives from these organisations to agree where responsibilities lay in relation to data protection and GDPR, sharing data securely and that relevant information is made available.

The Adult Learning team and providers are required to manage data protection to meet the standards of the Service, LBM, the Education and Skills Funding Agency, and the Greater London Authority, and their responsibilities under this policy. This policy will be reviewed as necessary in consultation with the affected personnel and representatives. Any changes to it will be made available to all affected by its provisions.

Introduction

MAL uses personal information in order to carry out the functions of the service as required by the GLA, the ESFA and law. A large number of Acts of Parliament and Regulations made under them requires and sometimes empowers MAL and the Council to provide goods and services to the community and to individuals in the community.

MAL will endeavour to ensure that it uses personal information in line with the expectations and interests of its customers, the Data Protection Act 1998, and the guidance for GDPR.

The Data Protection Act 1998 has eight principles on handling personal data. Personal data covers both facts and opinions about individuals. The principles require that data must be:

- Obtained and used fairly and lawfully
- Used for limited specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date (if necessary)
- Not kept longer than necessary
- Handled in accordance with the individual's rights
- Secure
- Not transferred to countries without adequate protection for data

In order to comply with the Act you must do the following:

- Personal Information will be processed fairly and lawfully. Customers will be informed about how their information is used and shared. Information supplied in confidence will not be disclosed without consent, unless it can be shown that the sharing is in the overriding public interest.
- Personal Information will not be used for secondary purposes that are against the legitimate interests of the people it relates to, unless those

purposes are required by law or are in the overriding public interest.

- Only seek to obtain relevant information. Whilst records kept by LBM or a provider will be adequate to support and record our work, they will not be excessive.
- If you become aware that the information held is inaccurate or out of date appropriate steps must be taken to correct it.
- Personal information must not be kept longer than is necessary and a Records Management Function must be in place to support this.
- Any requests from those who want to exercise their rights to access information will be assisted by the London Borough of Merton Information Governance Team.
- Personal data will be kept securely with appropriate safeguards in place according to the information's sensitivity.
- Personal data will not be sent out of the European Economic Area without appropriate safeguards to protect the rights of individuals.

Collection of Personal Data and Fair Processing

The Data Protection Act requires that the collection and use of personal information is fair. For this reason information about how and why information is being collected and who it may be disclosed to, must be available. Information necessary to make our collection and use of that information fair and transparent must also be available.

There are occasions when this fair processing information will not always be available. The collection or disclosure of information where authorised or required by any enactment does not require us to make available information about how it will be used (this information being a matter of public record). However, we will always provide details of how we use personal data on request, unless to do so would prejudice a criminal investigation or place someone at risk of harm.

Sharing Personal Information

Depending on the original purpose for which it was obtained and the use to which it is to be put, information may be shared with a variety of services. It may also be shared, where necessary, with other organisations that provide services on our behalf. We will always seek to share information with partners for the benefit of service users unless legal restrictions prevent this.

In all of these examples the information provided is only the minimum necessary to enable the provision of services. We will inform customers about who their data is shared with at the earliest opportunity.

Personal information may also be provided to central government departments, where we are required to do so by law.

Information is shared with the Police, Customs and Excise, the Inland Revenue and the National Fraud Initiative to prevent and detect crime, prosecute offenders and assess taxes.

When we share personal information we will do so securely and in compliance with our information security policy, and within the guidelines of GDPR. We respect the privacy of service users, whilst ensuring that we use the information that we hold to provide the vulnerable with the protection that they need.

We expect our staff and those of our providers, to respect the confidentiality of information about individuals. Whilst we will support staff in taking decisions about information sharing in accordance with their professional judgement LBM may take disciplinary or legal action against those who wilfully misuse personal data for unauthorised purposes.

Rights of access and prevention of processing

The Data Protection Act and GDPR guidance gives details on an individuals right to access, and consent to the information we hold about them. This right is not absolute, information about third parties, information prejudicial to investigations or social work as well as legal advice may be withheld in accordance with the law.

MAL supports the right of individuals to know how we use their information and will be proactive in allowing people access to their files.

Requests to access information held about individuals needs to be supported by proof of identity and the appropriate fee and will be responded to within 40 days.

Misuse of Personal Information

It is an offence for a person, knowingly or recklessly, without the consent of MAL to:

- obtain or disclose personal data or the information contained in personal data,

or

- procure the disclosure to another person of the information contained in personal data.

Unless the disclosure:

- was necessary to prevent or detect crime; or
- was required or authorised by law

LBM will take action against anyone found to be supplying information to a third party or using information for their own purposes without the consent of the council, or a reasonable belief that they were working in accordance with the wishes of the council. Such offences are criminal offences.

The Adult Learning team will review any information on breaches of data protection regarding our learners or the contracted service with providers during monitoring meetings. Actions will be agreed to address any shortfall areas.

This policy is reviewed annually, or earlier should there be a significant change to guidance or policy.