



MIAP
Managing Information
Across Partners

Learner Registration Service - Managing Your Users

Version 4

November 2009



Contents

Contents	2
1 Introduction	3
1.1 Purpose	3
1.2 Audience	4
1.3 Scope	4
2 Operational Arrangements	5
2.1 A Central User Administration Model	5
2.2 A Distributed User Administration Model	6
2.3 Set Up User Administration Procedures	6
3 Super Users	7
4 Creating users	8
4.1 Who Authorises the Request?	8
4.2 What Details are Recorded?	9
4.3 User Responsibilities	10
4.4 Arrangements for Data Governance	10
4.5 Training and Awareness	10
5 Updating Users	11
6 Access and Password Problems	11
6.1 Resetting a User Account	11
7 Removing Users	12
8 Monitoring Users Activity	12
9 Keeping in Touch	12
10 Special cases	13
10.1 Contract staff or third party organisations using the LRS	13
10.2 Lost your only Super user account	13
10.3 Awarding Body Role	14
10.4 Learner Plan	14
10.5 Personal Learning Record	14

1 Introduction

1.1 Purpose

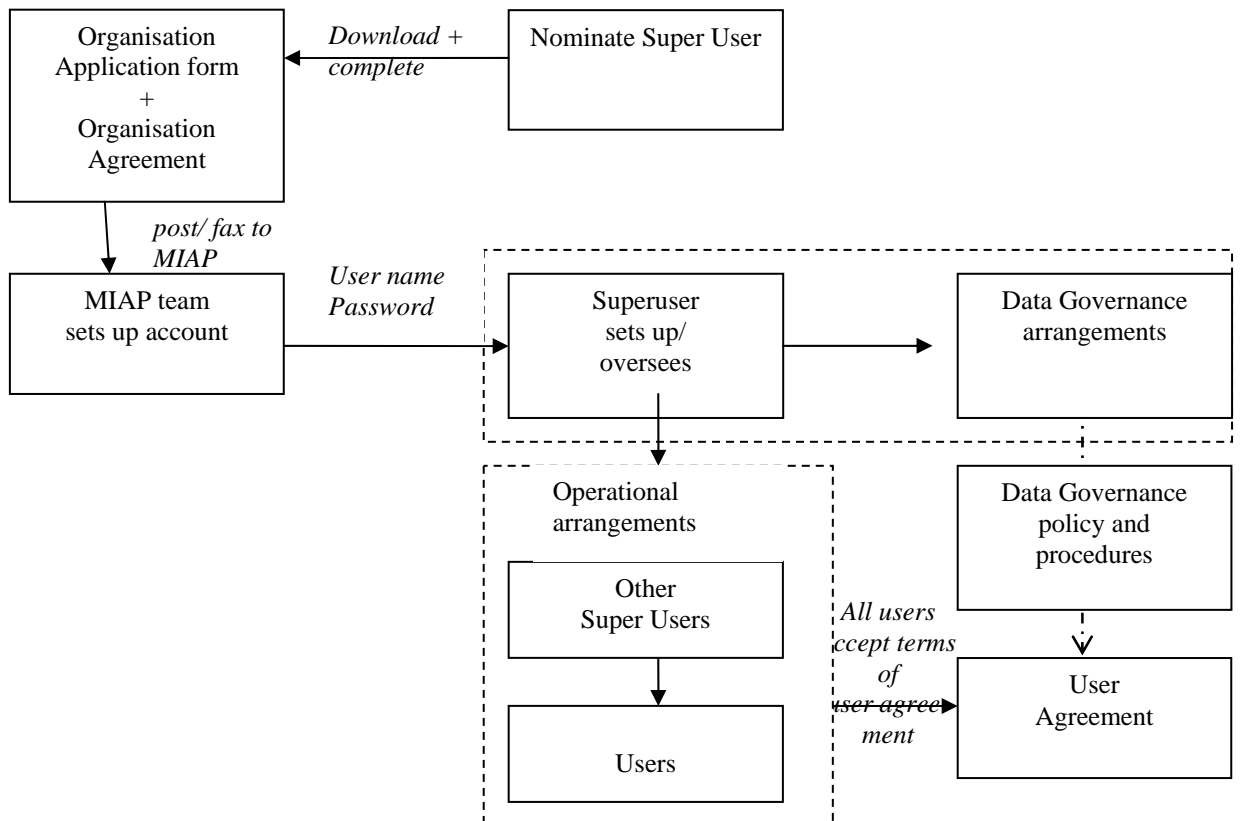
Having completed the one-off sign up process, as a Learner Registration Body (LRB), you will need to establish managerial arrangements for running the Learner Registration system and ensure that appropriate arrangements for data governance are in place.

Upon receipt, checking and acceptance of the sign up documents, MIAP will have set up the provider's account on the system for you and returned a user name and password to the Super User to enable access to the LRS portal and get started.

This guide is intended to help you from this single Super user starting point to:

- Clearly define your managerial arrangements for running the system
- Establish your data governance arrangements
- Assign additional Super User(s) and appropriate access for other users of the LRS

The steps you will undertake are illustrated in the diagram below:



1.2 Audience

This document is intended for organisations that are registered on the Learner Registration Service (LRS) and the super users within that organisation who deal with user administration.

1.3 Scope

This document is not intended to describe the functions of the LRS. This document only covers guidance on the Super user's role and the user administration procedures.

For further information refer to:

- The LRS Organisation Agreement
- The Organisation Registration Form
- The User Agreement
- MIAP Data Governance guidance
- MIAP website
- LRS Demonstration tool: Managing users

2 Operational Arrangements

This document deals with the user administration for a single MIAP registered organisation. The majority of registrations will be for a single legal entity even if you have multiple sites with users to manage.

When you first registered, MIAP will have set up your initial super user using the details you supplied to us on your MIAP Organisation Registration form.

From this single user starting point you must decide how to administer your user community and set up all other users.

The Organisation Agreement broadly sets out two complimentary areas of responsibility which might be expected to attach to the Super User(s) of the LRS:

- Oversight of Data Protection (DP) issues
- Operational management of the system including managing users, removing those who leave and oversight of procedure and practice.

It is commonplace, but not universal amongst providers, for the two to sit together in a single job role. For example, typically the role of the Super User within a college is a senior operational-level manager within MIS.

Your organisation may wish to consider creating additional Super Users if:

- Data protection responsibilities are separated from operational information processing management
- The potential number of learners or users is substantial
- The institution wishes to spread the risk / share the knowledge / provide staff cover
- Your organisation structure and locations

Having a single registered organisation entity within LRS does not prevent you from choosing to assign Super users for the different locations or to manage centrally. You need to decide who in your organisation is given the responsibility to manage users. This will depend very much on your internal organisation structure.

2.1 Central User Administration Model

For example; user administration can be part of a HR function, so that any new employees or changes in role are dealt with by HR and HR then applies system access changes as a result. In this example HR as a central team of super users is suitable.

OR you may have an IT or business support department who manages your systems for your organisation and the members of this team will become super users and deal with LRS user administration tasks.

2.2 Distributed User Administration Model

An alternative is a more distributed approach; if in your organisation the different geographical sites have their own business structure and a capability to manage their own user community at each site, then you might choose to assign a super user(s) for each site (or for a group of sites).

But beware! with this distributed model your Super users are NOT restricted by LRS to only the users at your geographic site but are given access to ALL users within your organisation.

Batch Files

With this being the case, you need to consider how to manage batches within your organisation. We recommend that you agree that each site has it's own name which can be input in the FileName field when submitting a batch. With the option to filter available on the Job Details screen, when a user logs on they can apply a filter that will only show the FileName they chose. Once set this will be applied every time they log on until they remove it. You may want to consider issuing guidance to all your organisation's users regarding the use of this functionality.

2.3 Set Up User Administration Procedures

Whatever your approach it is recommended that you appoint at least two more deputy super users to cover for absence and access problems of another super user.

In setting up your LRS user community you must also consider the internal procedures you need in place for employees to apply for access and to apply for change of role etc. You must also provide to your users the contact details of your super users in the event of problems. Remember your Super users must be the first point of call before contacting MIAP help desk. In small organisations where the staff are known personally to each other then a more informal verbal request approach may be enough. But if you have a large organisation you may need a more formal written application and approve model to manage your users.

The number of other users that you as a Super user may wish to create will reflect the extent to which enrolment and data entry are distributed within your organisation or managed centrally (see section 4 Creating users for more details).

Key points:

- 1. Decide how many Super users you need and where they are located (office wise).**
- 2. Set up and make known your procedures for requesting LRS user access, and changes to LRS users.**
- 3. Make sure your user community know your internal contact details for LRS support.**

3 Super Users

LRBSuperUser is the highest level organisation specific role that you can be given. As a Super user you are responsible for managing all users within your registered organisation. You can create other Super users for your organisation and it is recommended that you have at least two deputies. This role purely deals with user administration and not learner management functionality. If you want your user to do both a user management and a learner management role you will need to mix the LRBSuperUser role with one or more of the other roles available.

As written down in the MIAP LRS Organisation agreement your organisation is responsible for managing its own user community. This responsibility is done by the nominated Super users. This responsibility is in place to make sure that only the right people have access to LRS, that you maintain your user community and to make sure that the confidentiality of the records of learners is protected.

As a Super User you will be the first contact point for your user community for the following actions:

1. Creating users
2. Updating users
3. Access and password problems
4. Removing users
5. Monitoring User activity

Key points:

4. Users in your organisation must contact your super users first before referring to the MIAP help desk for assistance.

Your responsibilities in each of these areas are described in the next sections of this document.

4 Creating Users

As a Super User creating users, you must consider:

- Who authorises the request?
- What level of permission is needed for the user?
- What details are recorded for each user?
- And making sure that users are aware of their responsibilities in using LRS.
- Training and awareness on LRS including guidance on the use of the FileName field in respect of batches

4.1 Who Authorises the Request?

Any application for a new user account must follow your own internal process for checking persons who are being given access to confidential student records. Depending upon the role the person is taking this may involve CRB checks. CRB checking is NOT mandated by MIAP. You must set up procedures for requesting a new user account which checks that the person being given access is properly authorised to access the LRS.

In some cases you may employ temporary or short term staff. The procedures may be different for these users (for example CRB checks would too long and costly to do) and your procedures must consider this (see special cases section for further details).

MIAP does not recommended the creation of 'Guest' user accounts. This will break the responsibility for maintaining access authorisation . If you cannot be certain who is logging into the LRS then this can lead to a break in the confidentiality of the learner information within LRS.

What level of permission is required?

In order to protect LRS and the learner information it is your responsibility to make sure that people only have the suitable level of access needed for their role. In order to help this LRS provides a list of roles which you can assign to a user. These are:

LRBSuperUser – This is the highest level organisation specific role that you can be given. As a Super user you are responsible for managing all users within your registered organisation.

LRBOnlineUser – This is a basic role giving the user access only to the online capability for finding, registering and updating learners.

LRBBatchUser – This is a basic role giving the user access to submit batch jobs and to view the results and progress of your organisation's batch jobs.

LRBViewOnlyUser – On occasions you may want to allow someone access to find learners but not give them any power to register or update the learner records. This is the lowest level of access defined for the system.

AwardingBodyuser – See Awarding Body section.

LearnerPlanuser – See Learner Plan section.

LearnerPlanViewOnly – See Learner Plan section.

LearnerRecord – See Personal Learning Record section.

A user can be given multiple roles by choosing more than one role. You must assign at least one role when creating a user account.

4.2 What Details Are Recorded?

Aside from role the LRS can capture the following details for a user account:

- Title, Given name and Family name - LRS automatically produces a user account name from the characters of your given name and family name.
- Telephone number, mobile number – these fields are optional but can be useful contact details for the person.
- Email address – LRS will use this address to send forgotten password messages. MIAP recommends that you capture their email address.
- Preferred Language – tells you the language the LRS screens will be displayed in. Currently only English.
- Verification provided – confirmation of your internal authorisation procedure.
- Staff ID or Your reference – optional field which can hold an internal staff reference which can help with Employee identification.

It is NOT recommended that you name user accounts with generic names (for example 'User 1' or 'AdminDepartment') as these accounts cannot be associated to a person and as a result it is difficult to know who is accessing the service. If MIAP contacts you to talk about any user's unsuitable behaviour we may identify to you the user name that is causing the problem or behaving inappropriately.

4.3 User Responsibilities

Now each time you log on, every user will be presented with the User Agreement text.

This sets out the individual's responsibilities in using the LRS and must be accepted before access is given by the system. The user agreement text is also available within the LRS help pages for the system and on the MIAP website – www.miap.gov.uk for reference.

You may also want to reinforce this with your guidance notes or through training and awareness.

4.4 Arrangements for Data Governance

The MIAP requirements for data governance are articulated in the Organisation Agreement, while the obligations upon each individual user are set out in the User Agreement. These documents (available from www.miap.gov.uk), taken together, frame and detail the responsibilities imposed upon the provider. Ensuring proper practice in the handling of personal data is a requirement of learning providers although there is no standard model of practice across the sector.

4.5 Training and Awareness

MIAP gives no training courses in using MIAP. The responsibility for user training and awareness lies with your Super user. MIAP, however, does give a range of support materials (such as this guide).

MIAP will not be able to tell your users about your specific practices in the way you use LRS. This training must come from you.

Key point:

- 5. Make sure you have internal procedures for authorising new user accounts**
- 6. You need to consider if you want to give you own training and/or refer your users to the suitable sources provided by MIAP.**

5 Updating Users

It is important to maintain your user community. Your Super User can update and manage all your user account details. There are different update scenarios to consider...

- Change in details, name, contact numbers etc
- Change in role or permission

Basic account details, name, contact numbers can be maintained by the user. As a super user you can tell your user community how to maintain their user account.

You need to set up your procedures for authorising any changes in role, and make this known to users. This is important especially if the change gives the user more responsibility and access. You must make sure that your internal procedures cover any more checks needed before giving access.

6 Access and Password Problems

As a Super user, you are your user community's first point of call for:

- LRS access problems.
- Password resets.
- Suspending and reinstating access to a user account.

Whenever you receive an LRS access problem you should first find out if the problem is local access or internet connectivity problem before contacting MIAP.

6.1 Resetting a User Account

When a user has failed to access LRS due to a password problem and repeated tries to access then the LRS will 'lock' the account. The following process applies for resetting a user account:

1. Access the user account and change the status to active to reinstate the account.
2. The account is now active again and the password will work. You can tell the user how to receive an email prompt for their password from the LRS. This removes the need for you to know a user's password.

If a user (for any reason) is to be denied access to LRS then you can change a user account status to suspended.

7 Removing Users

It is important that you do not leave redundant user accounts with access to LRS against your organisation.

If a user account is left active a person after they have left can gain access the service from any internet capable device and potentially misuse the service. These activities WILL still be associated to your organisation and you will be held responsible!

Remove a user account when they have:

- Left your organisation.
- Moved to another separately registered MIAP organisation.
- Have taken on a role that no longer needs access to LRS.
- No longer being sub-contracted to by your organisation.

Key point:

7. Remove redundant user accounts as soon as possible.

8 Monitoring Users Activity

From time to time it is recommended that you take an audit of your user community to check if the users are still using the system and if they have the right level of access.

MIAP can provide you with a list of all your organisations registered users simply leave the Find user criteria blank and select all roles. MIAP cannot give an audit of your user's activity in the system.

9 Keeping in Touch

The initial Super User you gave us on your organisation application form is MIAP's primary contact point. If you change Primary contact point (this is normally your initial Super User) or your primary contact point leaves please tell the MIAP Help Desk of a change in your primary contact point so they you still receive updates on the service and the MIAP newsletter.

If any of your users wishes to receive the MIAP newsletter then they can

subscribe by sending their full name, organisation name and contact details to newsletter@miap.gov.uk.

10 Special cases

10.1 Contract staff or third party organisations using the LRS

From time to time you may hire contract or temporary staff to help within your organisation. As part of their role they may need access to LRS. These people should not be treated any differently to other users. In other words they must be subject to the same checks that protect confidentiality following your organisation's policy for this (it could be they may be too short in duration to warrant CRB checking)?

If another organisation is contracted to do work for your organisation that needs access to LRS, then it is your responsibility to give them access as users belonging to your organisation.

This will make sure that all transactions that are conducted for your organisation are audited as belonging to your registered organisation. After the contract ends you will still have access to the data (for example Batch jobs). At present contract organisations are unlikely to pass the MIAP registration checks to register directly as an LRB.

If you are an agency working for a number of different MIAP registered organisation you will have to use separate user logons for each organisation you are working for.

10.2 Lost your only Super User Account

In the unfortunate event that your Super User account is suspended or your Super user account holder has left, and you have no other Super user accounts available to access LRS, then MIAP will create a new Super User account for you.

In order to request a new super user please fill in the New Super User Form (available from the MIAP website) and send the form to MIAP. As MIAP is taking responsibility for granting someone Super User access for your organisation, the form must be approved by a senior manager within your organisation (preferably the same person which originally signed your Organisation Agreement).

10.3

Awarding Body Role

This role is only available to Awarding body organisations and will provide access to functionality specifically for Awarding body users. It allows access to the Verify ULN functionality using Verify Single Learner or the option to verify learners using batch.

10.4 Learner Plan

There are two additional roles which have been defined to give access to Learner plan functionality; Learner Plan and Learner Plan View Only. These roles are only available to organisations delivering learning to offender learners who have been approved by OLASS.

10.5 Personal Learning Record (PLR)

This role is only available to organisations who have expressed an interest in being part of the Personal Learning Record roll out and been accepted. This role will grant access to viewing and printing the personal learning record for any ULN.

It allows the User to access a learner's Personal Learning Record after a Find search has been performed.



MIAP
Learning and Skills Council
Cheylesmore House
Quinton Road
Coventry
CV1 2WT

T 0845 019 4170
F 024 7682 5681
www.miap.gov.uk

Publication code: **USR04 Version 4**