Skills Funding Agency

Learning Records Service

Code of Practice for Sharing Personal Information

Skills Funding Agency

Contents

Skills Funding Agency

Skills Funding Agency

Skills Funding Agency

1. Introduction

This Framework Code of Practice for Sharing Personal Information, herein referred to as "the Framework" has been developed to ensure that the requirements placed on any organisation using personal information generated and managed through the Skills Funding Agency's "Learning Records Service" (LRS) and the "Qualification and Credit Framework" (QCF) are legal, ethical and that the interests of the individuals whose personal information has been entrusted to these organisations are served.
This framework has been written with reference to guidelines and documents issued by the Information Commissioner's Office and relevant legislation.
Under section 537A of the Education Act 1996 as amended there exists a "Prescribed Persons List" (PPL) which provides lawful access to education data by those organisations listed. Together with the educational organisations that are allowed access for legitimate reasons, this document ensures that there is a code of practice that is consistent for all parties in respect of handling and managing personal information collected and stored as part of the QCF and LRS.
Facilitating a common approach to data sharing amongst all parties the code of practice forms both the basis for any data sharing agreements that may be made in the future and acts as "layer 3" of the official privacy notices for the Learning Records Service.
As a pubic initiative, any information collected and used may be disclosable under the Freedom of Information Act 2000.
This document will be subject to regular review at a minimum of every twelve months from the date of acceptance of the current published version.

1.1. The framework aims and scope

This framework code of practice is intended to fulfil the following functions:

- Functions as the 2nd and 3rd tier of the Learning Records Service Privacy statement.
- Formalise the approach to information governance and the sharing of data between organisations, both internal and external.
- Provide a foundation where formal sharing of data can be reviewed and enhanced with reference to common requirements and aims.
- Formalise document data sharing guidelines in accordance with Information Commissioner requirements and relevant legislation.
- Ensuring that the benefits of information sharing are delivered whilst maintaining public trust and respecting personal privacy.
- To ensure that by using this framework all parties share and manage personal and sensitive information legally and ethically and understand the implications of any mismanagement.
- To provide detailed information to the public who has an interest in how personal and sensitive information is managed as part of a layered privacy notice.

This framework code of practice does not fulfil the following functions:

- It does not act as a formal agreement for the sharing of information between public organisations. This will be done via separate Operational Level Agreements (OLA).
- It does not govern data sharing with third parties who are not involved in the system or recognised as “prescribed persons”. A separate “Third Party Data Sharing Protocol” document exists for these purposes.

This framework code of practice does not try to replace any decision making processes of the LRS or QCF in respect of data sharing. Rather it aims to provide a practical framework that can be used to guide decision making and reassure the wider public that good data management is of critical importance.

1.2. Learning Records Service

The LRS creates a Unique Learner Number (ULN) for every learner and the information used to generate this number will be stored as part of the Personal Learning Record (see below).

Use of the data collected for the ULN will be shared amongst education agencies in order to provide information to further the provision of educational services.

1.3. Qualifications Credit Framework

The creation of the Personal Learning Record (PLR) is administered by the QCF. This information is created and supplied under restrictive conditions to ensure that only those organisations that have access to the information are provided with it.

2. The law – the basis for data sharing

This section deals with the legislation that affects the sharing of personal and sensitive data, the guidelines, challenges, and issues in ensuring that the process of managing personal and sensitive data is done legally and ethically, yet aid’s the use of the information by all parties entitled to see and use it.

2.1. Legislative background

The basis for the collection and processing of personal, sensitive personal and confidential information are the following:

- Data Protection Act 1998.
- Sec. 537A of the Education Act 1996 which relates to the provision of information about individual pupils.
- Regulations made under Section 537A comprising the Education (Individual Pupil Information) (Prescribed Persons) Regulations 1999 and a series of amending regulations up to 2009 (the “Prescribed Persons Regulations”).
- Relevant legislation in the devolved administrations
- The Apprenticeships, Skills, Children and Learning Act 2009.

It must also be noted that with respect to information in general, any public organisation including the Skills Funding Agency are subject to the Freedom of Information Act 2000

and information that is not of a personal or confidential nature, or which cannot be exempted under the Act will have to be disclosed.

2.2. Data Protection Act 1998

The processing of personal information in the UK is governed by the Data Protection Act 1998. The tenet of the Act is the eight data protection principles, through which all controllers of data must manage personal information.

More information can be found in the Act itself, but below is a summary of the principles.

2.2.1. Data Protection Act 1998 - Principle 1

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

For the purposes of processing education information of a personal nature, the schedule 2 condition fulfilled is "the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms of the data subject".

Other conditions may be fulfilled depending on how the personal information is to be used and those affected by the use of their information are entitled to be informed about the use of their personal data and how it is held. This is done by a Subject Access Request (SAR), see below.

The purposes for using personal information are defined in the Awarding Organisation Agreement and the rights and freedoms of the data subject (the individual) are upheld.

2.2.2. Data Protection Act 1998 - Principle 2

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

The purpose of the collection of personal data and the uses to which those data are put are both lawful and fully disclosed in documentation that enables the LRS and QCF to function.

This principle ensures that personal data are only used where the use is lawful.

In terms of information that is used to create and populate the ULN, this information is already collected by the Skills Funding Agency and as such may be shared for educational purposes commensurate with the original purposes for which they were collected.

The information used to create the Personal Learning Record which is allied to the ULN but uses information collected by awarding organisations and educational institutions, has a greater level of restriction placed on it and is governed by operational agreements and/or contracts; whichever is suitable to ensure that information is only used for the purposes it was collected. This information may only be used to administer the PLR and be used by the learner to whom it belongs, to manage access to it by others, e.g. prospective employers.

2.2.3. Data Protection Act 1998 - Principle 3

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."

The requirements for all personal data will be justified; no information will be requested from individuals unless there is a lawful, legitimate reason to request it.
Enough information will be required to ensure that individuals are not mistaken for others with similar details, for example the same name, and equally information will not be collected unless it is not required for the purposes directly related to the provision of the services offered.

2.2.4. Data Protection Act 1998 – Principle 4

"Personal data shall be accurate and, where necessary, kept up to date."

The records containing personal data generated by the Learning Records Service and contained in the Personal Learning Record will be available to the individual learners and may be amended, or requested to be amended, if inaccurate.
The Awarding Organisation and where relevant the associated centres that submitted the data will be responsible for maintaining personal data that they have collected, on an ongoing basis.

2.2.5. Data Protection Act 1998 – Principle 5

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

Individuals may wish to continue learning and studying throughout their lives and have the need to review and prove the qualifications they have attained at any point in their working lives.
It has therefore been agreed that the retention of personal information will be a minimum 66 years, providing for a level of certainty that information important to the individual will be accessible throughout their life.

2.2.6. Data Protection Act 1998 – Principle 6

"Personal data shall be processed in accordance with the rights of data subjects under this Act."

Privacy notice guidance will be available to all Awarding Organisations as part of the Skills Funding Agency's obligations as data controller. Organisations will be encouraged to ensure that their Privacy Notices reflect the requirements of data collection for services that the learner will be provided with.
The Privacy Notice guidance will help to describe the services (allocation of a Unique Learner Number and creation of the Personal Learning Record) and the data collection requirements including the reason for use and any proposed sharing of the personal data that will take place. It will also identify the process by which learners may opt out of having their data shared, where this is permissible.

2.2.7. Data Protection Act 1998 – Principle 7

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

All measures required to ensure the security of personal information will be taken in all aspects of the system processes and a security policy will be in place that details the steps being taken to comply with this principle of the DPA.

2.2.8. Data Protection Act 1998 – Principle 8

"Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

Whilst the DPA provides for the movement of personal data inside the European Union, there are no intentions to share data outside of England, Wales, Scotland and Northern Ireland.

2.3. Data Controllers

A data controller is defined by the Data Protection Act 1998 as someone (an organisation or a person) that either alone or jointly, or in common with others "determines the purposes for which and the manner in which any personal data are, or are to be, processed".

The data controller for the creation of the Unique Learner Number and the subsequent management of personal data in the Personal Learning Record will be the Skills Funding Agency. However, the Awarding Organisation that is responsible for awarding credit and qualifications to learners will also be a data controller in common with the Skills Funding Agency.

A data controller "in common" indicates that the two, or more, data controllers have autonomy to use the personal data collected for any purposes within the defined reasons for which the data have been collected initially. It is important that data controllers in common understand that any breaches of the DPA are their sole responsibility unless the breach has occurred due to more than one organisation's involvement.

This is different from joint data controllership in which liability is joint and the data collected will be used for the same purposes. This joint relationship may exist with some LRS partners with whom data are shared on a highly defined basis with suitable restrictions.

The LRS share data in three particular ways:

- Receiving from and passing to Awarding Organisations
- With known partners under operational agreements
- With third parties via the LRS Third Party Data Sharing Protocol.

Due to the complex nature of data sharing and the way in which organisations may control data, the type of data controller is not fixed, but in general terms will be a particular data controller relationship for each method of sharing.

2.3.1. Receiving from, and passing to Awarding Organisations

The Awarding Organisations updating the Personal Learning Record are responsible for maintaining their own achievement data on their own systems. The obligations of the Awarding Organisation as a data controller and its use of the data from the PLR for the QCF are defined in the Awarding Organisation Agreement. In summary Awarding Organisations are only permitted to process the data accessed via the PLR for the following purposes as per Schedule One of the Awarding Organisation Agreement:

- To confirm that a learner can transfer credit using the credit check function
- To support the process of determining a potential award of a qualification to learners
- To verify prior attainment
- To monitor progression, success and pathways through undertaking a single qualification credit check query or a Routes to Achievement query
- Identifying possible errors in the data

- To provide information, advice and guidance to learners

Any organisation deemed to be a data controller in common (or otherwise) with the Skills Funding Agency will be expected to take all measures possible to comply with the DPA and other legislation and where information held by the Agency is involved will take any measures required, as specified with the Security Policy.

Other expectations of Awarding Organisations are that they will maintain the currency of their data contained in the PLR in line with any participation agreement parameters; the current expectation being no longer than ten days after updating the data in their own systems.

2.3.2. Shared with known partners

There are a number of organisations with which the LRS needs to share learner information in order to provide educational services and manage education nationally. These are known partner organisations and are generally on the “prescribed persons list” which is based on the list of organisations that can access educational data under the Education Act 1995 (as amended).

Learner information shared with these organisations is done so under strict “operational agreements” which govern the uses of the data being provided.

Due to the nature of how the learner information is used, the partners assume a level of responsibility for those data and as such are “data controllers in common” with the LRS which means that each organisation is responsible for managing the learner data in their care.

2.3.3. Third parties via the LRS Third Party Data Sharing Protocol

Requests for learner data from organisations which may not be known to the LRS or which may be requesting one-off or novel data will be subject to this protocol.

Depending on the use of the information requested, the third party may be a data controller in common or a joint data controller with the LRS. This will be determined based on the request and to ensure the best possible protection of learner data.

Regardless of the data controller type, the LRS reserves the right to provide learner data with specific restrictions or requirements which it believes will help to protect learner data from deliberate or inadvertent abuse.

2.3.4. Skills Funding Agency

In operating and maintaining the systems that create and manage the ULN and PLR the Skills Funding Agency will be a data controller and is obliged to comply with all requirements, both internally agreed and externally issued, to ensure the safe and good management of all personal data in its care.

2.4. Data Processors

Data Processors process personal data *on behalf of* a data controller and where this relationship is necessary, the data controller will ensure that agreements are in place that require the data processor to fully comply with the DPA and any other guidelines and legislations that may be appropriate.

In the event that processing is required by a third party that is processing data that is not entirely on behalf of a data controller, then the relationship will be that of joint data controllers, but with the Skills Funding Agency or Awarding Organisation taking the lead and accepting joint liability or by requiring the third party to agree to conditions in an agreement referring to the "Third Party Data Sharing Protocol" in order to assure users and management that the sharing is legitimate, controlled and fully within the bounds of acceptable use.

2.5. Privacy Impact Assessment

There is a requirement for Government projects and systems, as published by the Cabinet Office, to undergo a Privacy Impact Assessment (PIA). A PIA is "*a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a search is undertaken for ways to minimise privacy concerns".*

A PIA has been conducted and recommendations from the final report will be incorporated into an ongoing improvement programme of the systems and processes. All PIA work undertaken has been based on the PIA Handbook and more information about PIAs can be found at the Information Commissioner's Office website at https://ico.org.uk/.

Skills Funding Agency

3. The approach to consent and fair processing

A significant amount of the data management for the LRS and QCF processes is performed under the DPA by way of it being a legitimate use of such data for the services provided.
However, access to personal information by third parties is dictated largely by consent given or withheld. These processes have been determined and agreed with the Information Commissioner's Office.

3.1. Unique Learner Number

The Learner Registration Service allocates the ULN for each learner at the appropriate time via systems into which education institutions enter the learner details.
Due to the nature of the ULN and its importance to the learner throughout their education, and potentially through their work lives, the allocation of the ULN is compulsory and the learner cannot opt out of providing the minimum information necessary to allocate the ULN.
ULN and associated information may be shared, with conditions, amongst Learning Records Service partners and used for statistical and research purposes.

3.2. Personal Learning Record

The Personal Learning Record, created from the ULN and the achievement and participation information provided by education institutions and awarding organisations contains personal data from a number of sources:

i) Key Stage 4 and Key Stage 5 data received from the Department for Education "National Pupil Database" ii) Participation and achievement data received from the Skills Funding Agency
Individualised Learning Records returns iii) From Awarding Organisations who collect achievement data relating to learners who have achieved an award with that Awarding Organisation – subject to strict controls and agreements.

All learning events are validated before being loaded into the PLR and this validation includes the ULN and key personal details in order to ensure that no personal details are confused or inaccurate.
All information provided will be either personal or non-personal data. No sensitive personal data such as those data relating to ethnicity, religion, health, sexual life or political opinion or court proceedings will be provided. This process creates a useable PLR for each individual learner under secure conditions.
PLR information is tightly controlled and the restrictions placed on this information mean that information access may not be possible, or require high levels of justification before it may be shared.

The learner is provided with the ability to refuse their consent in respect of having any achievement and participation data from their Personal Learning Record passed to third parties, including those listed at www.learningrecordsservice.org.uk. Details of opting out

may be found on the website or by telephoning 0845 602 2589, where their wishes will be recorded on their record.
It is the prerogative of the learner to change their consent at any time. The above mechanism also provides for learners to give consent to share information. However, it must be noted that if consent is initially given and then revoked any data shared up to that point in time will remain useable where it has been shared, but no new data will be released. The Privacy Notices issued for the services will inform learners and any other individuals where their information may be shared and these will be updated periodically to reflect any changes.

3.3. Sensitive personal data

Sensitive personal data, as defined by the Data Protection Act 1998, includes:

- Racial or ethnic origin
- Political opinions
- Religious beliefs, or other beliefs of a similar nature
- Trade Union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Proceedings for any offence or alleged offence

Sensitive data issues may occur for two reasons; firstly data items may inherently be sensitive or indicate certain attributes of individuals, secondly the sensitivity may be “sensitive learning events” regarding the identification of certain individuals, such as vulnerable learners, VIPs or offenders.
The LRS and QCF collect only the information that is required to enable improved services to learners and manage the existing service. However, in an environment that is complex to manage, some sensitive personal data may be included in a learner’s records.
In these instances the information will be managed through a number of controls both to try to prevent the inclusion of sensitive personal data and if it should be identified, to control the release and use. Dialogue regarding these risks have been discussed in depth with the Information Commissioner’s Office.

3.3.1. Self-notification by a learner

Where a learner is concerned about their personal information held in the LRS/PLR they can invoke one or more of the following approaches to address any concerns that they may have.

1. Initiate a data challenge via the system facilities (online).
2. Change their “consent” status via the flag available online, or via the Customer Helpdesk and “opt out” of sharing their achievement data.

3. Contact the Helpdesk to review the terms of the privacy notice that they were presented with when they registered. This is part of the data challenge procedures and will be managed by the Customer Helpdesk through a set of operational procedures.
4. Make contact with an authorised body or their learning provider and request that they deal with the LRS directly, on their behalf.
5. Contact the Skills Funding Agency in writing at the address given on the Skills Funding Agency and LRS websites.

No reason is required to be given by the learner to justify their enquiry or challenge. However, the LRS will require a minimum set of information to be provided to allow it to take appropriate action. As a guide, the LRS will deal with any issues raised as described in the table on the following page;

Table 1 – Managing sensitive personal data

	Learner Register Record	Personal Learning Record	Learner Plan
Learner Deletion	N	N	N
Learner Update	Y	N	N
Learner Registration Body Deletion	N	N	N
Learner Registration Body Update	Y	Y	Y
Authorised Body Deletion (*)	Y	Y	Y
Authorised Body Update (*)	Y	Y	Y

3.3.2. Participation and achievement data controls

A number of controls exist in respect of participation and achievement data because of the nature of how these datasets are created. These include:

Restrictions on free text input values

There are rules that apply to free text areas of the PLR. For example it is not possible to enter “criminal” into any free text field in the PLR. Such restrictions reduce the risk of collecting superfluous or unnecessary data.

Restrictions on sensitive learning events

There are no text restrictions on data that may be entered within achievement and participation fields. However, there is a list of sensitive learning aims which is maintained by the learners, registered learner registration bodies and any stakeholder with legitimate interests. The list works by preventing third party access to specific records where the type of record is deemed sensitive.

Where a learner or LRB notifies the LRS of a learning event that they believe is sensitive, the LRS will carry out an investigation through the operational data challenge process. If accepted then all data for this type of event will become restricted for all learners affected.

Restrictions on learner plans

Fields within the system relating to learner plans are restricted where this might identify the learner as having offender status. These restrictions cover both demographic and participation records and are managed by the LRS Offender Learning team in partnership with National Offender Management Service (NOMS) and the LRS service.

Restrictions apply to UK provider reference numbers within the learner plans in order to prevent the identification of the place of learning.

3.4. Privacy Notices

The QCF and LRS have taken the decision to follow the Information Commissioner's advice and adopt a layered approach to privacy notices.

Privacy notices are the mechanism by which individuals are informed about what will happen to the data collected about them, how that data will be processed and shared and what processes exist for individuals to request changes or, if allowed, to stop certain aspects of data management taking place.

In certain circumstances the privacy notice may also serve as a means of obtaining consent to certain types of data collection and processing. A typical example being is a company wishing to send out marketing information, who may request a box to be ticked by the individual to consent to personal data being processed for this purpose.

The Information Commissioner's "Privacy Notices code of practice" provides guidance and recommendations which have been considered carefully in creating the layered privacy notices used by the Skills Funding Agency.

Layered privacy notices generally have 2 or 3 layers of notification.

The first layer notice can be brief and to the point, providing only high level information, but enough that most people can make an informed decision that their information is being used correctly. The first layer will then point to a second layer notice that is quite often a web page, e.g. https://www.gov.uk/government/publications/lrs-privacy-notices

The second layer contains more detail about how and why personal information may be processed. It contains specific information on third party organisations that may have access to data and why it is required. It also provides further information for the individual to make contact with the data controller so that they may modify their consent, should they wish to do so.

A third layer may be provided which includes more detailed information, e.g. relating to relevant legislation, regulations, policies and protocols. This document represents the 3rd layer of notification.

Not all organisations who themselves, or have learners who, wish to make use of the LRS and QCF services, are covered by the Privacy Notices issued by the Skills Funding Agency or the Department for Education. The LRS has developed standard text for these institutions to include in their own Privacy Notices.

Whilst making a learner aware that their data will be shared through the LRS/QCF is the responsibility of the registering/enrolling institution and not the LRS, it would be damaging to the LRS reputation if a learner's data was collected or shared in a way that was considered unfair.

It will be the responsibility of individual organisations to show a learner an appropriate Privacy Notice as part of the enrolment/examination process. The LRS requires that individual organisations include the first layer of the LRS Privacy Notice in their own privacy notice text. This will direct learners who require further information to the second layer on the LRS website. The LRS/QCF recognises however that it cannot be responsible for ensuring the learner looks at the privacy notice, as they did not issue it, are not collecting the data in the first instance, and are not managing the enrolment process.

The LRS recognises that those organisations who wish to use the LRS/QCF Service may have their own privacy notices that cover their own internal activities. However, to enable consistency across the sector, and as advised by the Information Commissioner's Office, the LRS will make available standard privacy notice text for use by organisations using the LRS/QCF Service.

It is the responsibility of the registering organisation to show the learner the privacy notice as part of an enrolment/examination process. The requirement for the LRS organisation user to issue appropriate privacy notices will be included in the usage agreements between the LRS/QCF and the registering organisation.

Standard wording that the organisation should use will be available from the LRS website.

3.4.1. Privacy Notice Recommended Text

The LRS provide two recommended sets of privacy notice text; extended text and shortened text. The following wording should be included in the Learning Provider's own privacy notices.

Text 1 – Extended Text

The information you supply will be used by the Skills Funding Agency to issue you with a

Unique Learner Number (ULN). This number will be used to create your own Personal Learning Record.
Your Personal Learning Record will include information about your qualifications, awards and training events and learning achievements which are part of the Qualifications and Credit Framework. It also means that information about your learning can be shared with others who have a responsibility for your education and training.
If you have still not reached the age of 16, you might first wish to discuss this Privacy Notice explanation with your parent or legal guardian. The Chief Executive of Skills Funding is the legal representative of the **Skills Funding Agency** which funds some of the qualifications and training that you may be receiving through your college, training or learning provider. Your Personal Learning Record will include information about your qualifications, awards and training events plus learning achievements that you may collect throughout your lifetime of learning – at all levels and also whilst you are working and learning.
The information that you provide to us will be passed to the Learning Record Service for the purpose of allocating you with a Unique Learner Number (ULN). This is a ten digit reference number and is unique and individual to yourself. Please keep this number in a safe place since you will need it during your lifetime, just like your National Insurance Number.

The Learning Records Service will also create your own Personal Learning Record (PLR). This record will include information about your qualifications, awards, learning achievements and 'credits' which will be conveniently located in one online area for you, and with your permission, your advisors to refer to,. Your record will help you to confirm to others, what you have learned, where and when. It will also help you identify other areas of learning to help you progress towards your own goals.
Please note that **you will always be in control** of who accesses your Personal Learning Record for the Qualifications and Credit Framework (QCF).Only you can give them permission to view the information.
Your Unique Learner Number (ULN) will also be used to collect and share information amongst education-related organisations. Such information includes qualifications, awards, certificates, work-based training and learning (this is also called achievement and participation data). Your Personal Learning Record will be a lifelong record of your participation, learning and achievement in education. Your Personal Learning Record will be accessible to you, plus to organisations linked to your education and any other organisations you allow to view your Personal Learning Record for the purposes of advice and guidance. This could include Next Step, careers advisors, college registration and course enrolment staff and future employers if you give them access.

Your Personal Learning Record allows you and other organisations to check your own learning 'credits' achieved. One of the long term key benefits is that it will help you see how well you are progressing towards your own learning outcomes, training or qualifications and help you find alternative ways of reaching your own learning goals. For

further details of how your information is shared and used by the Learning Records Service and how to opt out or modify who has access to your information please visit the Learning Records Service website at https://www.gov.uk/government/publications/lrs-privacy-notices

Text 2 – Shortened Text

The information you supply will be used by the Chief Executive of Skills Funding, to issue you with a Unique Learner Number (ULN), and to create your Personal Learning Record. Further details of how your information is processed and shared can be found at https://www.gov.uk/government/publications/lrs-privacy-notices

3.4.2. Second layer - Standard LRS privacy notice text

This statement is intended to provide you with information as to how the Learning Records Service (LRS) will collect and use your personal data, and how you can exercise choice in respect of the use of your personal data.
The LRS is operated by the Skills Funding Agency. The LRS collects data relating to learners registering for relevant post-14 qualifications, for example GCSEs, AS and A Level Qualifications, Diplomas and associated units, Apprenticeships, Entry to Employment Certificates and Qualifications Credit Frameworks and associated units.
The LRS offers two core products and functions:

- a Learner Register (Organisation Portal) which allocates a Unique Learner Number (ULN) to each learner
- a Personal Learning Record. The Personal Learning Record will offer the learner the facility to access their participation and achievement data via a website and will enable this information to be shared with other organisations and individuals as further explained below.

The LRS collects data from:

- information which is already being collected by other agencies from schools and other learning providers
- the information you provide when you register with a learning provider.

The LRS will collect and store the following information:

- Learner Register: The information that will be collected about each learner will be basic information about you as an individual, for example, your name, date of birth and postcode.
- Personal Learning Record: In addition to the above, the Personal Learning Record will also contain information about your educational qualifications, date of qualifications, courses studied and the place of learning.

Using the Unique Learner Number, LRS products and functions will enable organisations across the education and training sector to share information about participation and achievements in a consistent and approved manner, promoting good information management practice, and helping to improve accuracy and efficiency. This will benefit

the learner through ease of application to learning providers, better access to their information and the ability to challenge inaccuracy.
The Personal Learning Record will be shared with organisations linked to your education and training, including those organisations specified in Regulations made under section 537A of the Education Act. The Personal Learning Record also enables learners, if they so wish, to choose to share their participation and achievement data with other third parties such as prospective employers, as described further below.
All organisations that will have access to the information you provide are required to sign a data sharing agreement which requires them to manage your data responsibly and only to access information where there is a direct connection between you and the relevant organisation.
Visit https://www.gov.uk/government/publications/learning-records-service-awarding-organisations for more details about the Awarding Organisations agreement. At no time will your personal information be passed to any organisations for marketing or sales purposes.

Because the ULN is required for the administration of services within the education sector (such as the issuing of certain qualifications), individual learners are not able to opt-out of being included on the Learner Registration Service or being issued with a ULN.
Individuals can opt out of sharing their participation and achievement data through the Personal Learning Record with organisations linked to their education and training, including those organisations specified in Regulations made under section 537A of the Education Act. Details of how to opt out of data sharing can be found at www.learningrecordsservice.org.uk or by telephoning the Customer Helpdesk on 0345 602 2589. Please note that organisations may still share some data outside of the Learning Records Service.
Information will only be shared with organisations outside the education sector with the positive consent of the individual learner concerned, which can be given by the individual accessing their Personal Learning Record. Individuals have full control over what information will be shared as well as who it may be shared with. Full details of how to grant permission for sharing with third parties can be obtained from the customer helpdesk.
One potential consequence of deciding not to give permission to share the Personal Learning Record is that you may need to provide paper copies of certificates or other information to verify qualifications.
A major benefit of the LRS service is that you can check information held about you is accurate and request that any errors are corrected. If you believe that any information on your Personal Learning Record is incorrect then you should follow our data challenge procedure.
The LRS makes every effort not to collect any information which consists of sensitive personal data (e.g. data which relates to ethnic origin, physical or mental health, religious beliefs, trade union membership or any criminal offences or proceedings). If you find that any sensitive personal data has inadvertently been included, you should

contact the LRS. The LRS have a policy in place that controls the collection and use of sensitive data.
The LRS recognises that some learners have specific concerns about privacy which mean that additional safeguards are required. The LRS have a policy in place that controls the collection, use and management of data relating to “sensitive learners”.
The LRS recognises the need to keep your information secure and has implemented technical and organisational measures aimed at preventing loss of, or unauthorised use of your information.

The ULN and Personal Learning Record are intended to provide a life-long record of learning which will be available to you at any time you choose to participate in education or training. Therefore the LRS may continue to hold your ULN and associated data for at least 66 years, and beyond if the record is still active.
The LRS recognises that privacy and data protection concerns can evolve over time and will keep this policy under review. Any amendments will be posted here and will be notified to learners when they access their Personal Learning Record.

4. Data Sharing

Data that may be shared by the LRS may one of several types; anonymised, aggregated, de-personalised, or identifiable/confidential.
Each of the types of data will be managed in accordance with the best practices for securing the data and managing it responsibly, legally and ethically.
Requests for information from LRS systems may be made by any organisation that believes it has a legitimate right of access. However, unless the organisation is a known organisation, in that it has permission as part of its function to access data, then each request for information will be considered on its own merits and with regard to the "Third Party Data Sharing Protocol" which sets out the requirements that third parties have to fulfil in order to receive the data they request.
Even if the organisation fulfils the criteria and agrees to the Third Party Data Sharing Protocol, the Skills Funding Agency, as the data controller can still refuse access where it believes there may be substantial risk to personal sensitive or confidential information.

4.1. Anonymised data

Anonymised data are data where all identifying information has been removed. For example, name and address plus any potential data that may be linked to re-identify a person such as postcode and date of birth.
Properly anonymised data carries with it very little risk that the data may be matched in future to other information to identify the original persons. As such anonymised data is used wherever possible and where aggregated data is not sufficient for the purposes required.

4.2. Aggregated data

This type of data represents data that has been processed to produce a generalised/statistical result. For example a set of data may state that there are x number people living in Cheshire with a degree in History. From such information, it is highly unlikely that anyone could be identified either from the data or in the future if that data is added to other information to broaden, or narrow, the results.
The LRS recognise that in some aggregated cases there may be data that indicates a very small number of results, for example, the number of qualified
Neuro-surgeons in a small village. To this end and to protect individuals who may be identified against their wills in such small numbers, the LRS will decide on the appropriateness of releasing such information when these types of results occur.

4.3. De-personalised data

De-personalised are similar to anonymised in that personally identified data is removed. However, other data that may be used to identify an individual may remain in the dataset, such as postcode, date of birth and qualifications.
Because of this, de-personalised data is not considered anonymous enough to be sufficiently robust from future matching. Therefore datasets of this nature will require an agreement under the Third Party Data Sharing Protocol or other suitable agreement, for example the Awarding Organisation Agreement.

4.4. Identifiable/Confidential

Whilst identifiable and confidential information are often thought of as different types of data, they must be treated in much the same way. Both types of data will be subject to agreement by the requestor to the terms and conditions laid out in the Third Party Data Sharing Protocol and any other requirements as may be identified before the request is fulfilled.

4.4.1. Personal data

Personal data are data that identify a person or persons and so are subject, in the case of living individuals, to the Data Protection Act 1998. Any data which may be used either alone or in conjunction with other data to identify a person is identifiable data.

4.4.2. Confidential data

Confidential data may be identifiable data or non-identifiable data that carries with it an expectation that it will be secured and protected from those who do not have a right to see it. These could be documents relating to an organisation and be commercially sensitive.

To be considered confidential there generally has to be three criteria fulfilled, which are based in common law:

i) The information must have the necessary qualities of confidence about it ii) The information must have been communicated in circumstance importing an obligation of confidence

iii) The information should be clearly identifiable (in the context of where else it may be held) and original

These criteria were laid down by Mr. Justice McGarry in Coco v Clark (1969) and form the basis of the Common Law Duty of Confidentiality.

4.5. Charging for data

In certain circumstances, and where there are no legal requirements for data to be shared, organisations may have to place a charge for access to the requested data. Whilst this is not seen as a normal activity, it is understood that some requested data may be costly for the LRS to provide, or be otherwise difficult to produce.

In these instances, the organisations arranging data sharing agreements need to make suitable provision, if any charge for access to the data is to be made.

4.6. Sharing data for commercial purposes

Commercial use of data is mainly interpreted to involve marketing. However, marketing need not necessarily be for commercial purposes. As defined by the Data Protection Act 1998; “[marketing is] the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals”.

The concern with regard to commercial sharing is not with the data being received by a commercial organisation, but the processes and controls in place to ensure that data residing with a commercial enterprise cannot use that data for purposes other than those agreed.

As the potential to use personal data gathered by the LRS for commercial purposes increases, careful consideration must be given to the security and understanding of commercial enterprises and how sharing may affect the individuals concerned. The LRS

and partner intending to share data with commercial organisations must ensure that they have a right to do so.
Any agreements made between the LRS, its partners and/or commercial organisations must have in place a robust and fully agreed data sharing agreement that is signed and actionable by all parties. There must also be suitable clauses built into any contracts between such parties which fully identify liability and obligations to using the data for these purposes.

4.7. Cross border sharing

Cross border sharing encompasses the sharing of information outside the UK and also within the UK where devolved administrations exist.

4.7.1. UK Boundaries

There are four nations within the UK; England, Scotland, Wales and Northern Ireland. Some partners are based in different regions or have specific remits to provide services in one or more of these locations.
The Data Protection Act 1998 is a UK wide Act, but due to the administrative nature of the devolved nations it is important that data are shared and managed in accordance with any laws specific to those nations.
With this in mind the LRS will work closely with their counterparts in the devolved administrations to ensure that the sharing of identifiable personal data is done legally and ethically at all times.
If data has been gathered with the specific purpose of using the data only for the educational purposes in that area, then whilst the DPA will cover the movement of data, it is up to the group to decide how it will manage access to data that perhaps should not be used or processed by other regional departments.

Consideration will be given to the need to:

- Ensure that the potential sharing of data across regional boundaries with regional organisations is documented for the individual to be aware of, either via terms and conditions or by the option of giving consent.
- Manage at a local level between partners the access to data – this is what would be done now anyway, but will cease to be practical as and when a centrally managed data warehouse is operational.
- Manage access via the LRS. This could be very bureaucratic and lengthen data sharing times, notwithstanding that many partners would be unhappy about devolving data sharing to another party.
- Ensure that the party with whom data is to be shared is either:
  - A member of the United Kingdom Register of Learning Providers
  - Covered by regulations having effect in the appropriate nation
  - Covered by the appropriate consent of the learner whose data is proposed to be shared.

So long as it is made clear to individuals as to the fact that data may be transferred to regionally based organisations, then sharing should be able to take place as required, so long as the sharing remains in line with the purposes for which those data have been collected and within the confines of the DPA 1998.
Any restrictions on the movement of data in this way should be discussed and documented within data sharing agreements.
Note that the Isle of Man, Channel Islands and some other territories of Great Britain, are not part of the UK and may not be part of the EU. In these cases agreements made with government departments of these areas, may need to refer to legislation other than the Data Protection Act 1998. Additional safeguards may need to be put in place to cover these situations, such as, the use of standard contract terms approved by the European Commission for the transfer of data outside of the European Economic Area (EEA).

Wales

Powers in relation to sharing of individual pupil information in Wales were transferred to the National Assembly for Wales in 1999.
The LRS via the Skills Funding Agency is permitted under Regulation 5 of the Prescribed Persons Regulations (England) to share information with entities which are registered on the UK Register of Learning Providers (UKRLP), which may include organisations in Wales. This is believed to be sufficient to allow the LRS to share information with institutions in Wales, provided they are registered with the UKRLP.
The LRS is also permitted under the Prescribed Persons Regulations (England) to share information with the National Assembly for Wales and the Welsh Joint Education Committee (Regulation 4). However, the details of what information can be shared within
Wales is governed by a separate set of Regulations, the Education (Information about Individual Pupils) (Wales) Regulations 2007. These regulations are different to the equivalent English regulations and do not contain power to share information with all the categories of institutions referred to in the English regulations.
Consequently, the legal basis for the LRS to share information with institutions in Wales may be more restricted than in England. To the extent that a learner has consented to sharing of information through a relevant and sufficiently clear privacy notice, this is believed to be sufficient to justify sharing of ordinary personal data with an institution in Wales which is not registered with the UKRLP, but not any sensitive personal data (which would require explicit consent).

Northern Ireland

The LRS is permitted under Regulation 5 of the Prescribed Persons Regulations to share information with entities which are registered on the UKRLP, which may include organisations in Scotland and Northern Ireland.

There currently appears to be no provision in the Prescribed Persons Regulations for sharing of information with any authorities in Scotland or Northern Ireland. Consequently, the legal basis for the LRS to share information with institutions in Northern Ireland may be more restricted than in England. To the extent that a learner has consented to sharing of information through a relevant and sufficiently clear privacy notice, it is believed that this will be sufficient to justify sharing of ordinary personal data with a learning provider in Scotland or Northern Ireland which is not on the UKRLP, but possibly not any sensitive personal data (which would require explicit consent).

Scotland

As at October 2010, the Learning Records Service is not permitted to offer services in Scotland. Some cross border sharing of data is occurring, but this will be for learners undertaking skills courses in England.

International Boundaries

Principle 8 of the Data Protection Act 1998 states that “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.
The LRS is a UK wide programme and there is no intention to enable data to be transferred outside of the UK.
The LRS contractually binds the supplier not to transact data outside the European Union.
Personal data may be transferred to a non-authorised country in certain cases, such as:

- The individual explicitly consents to the data being transferred to a country or territory that has acceptable and recognised privacy arrangements or
- The data must be passed in order to fulfil a contract or obligation with the individual.

4.8. New uses for personal data

Regardless of whether an individual gives consent directly, or their consent to certain processing is built into the terms and conditions of a contract/enrolment the issue of foreseeing new uses of the data originally collected needs to be considered.
Data are collected and processed for specific purposes that should be documented or implied. New uses for data may be different enough not to be covered by the documentation when individuals agreed to have their data used.
A good example of this is the future use for marketing non-educational services via other government departments. For example it may be that a partner or other organisation with access to the data determines a new use. It is important that the individual can have reasonably foreseen this use in order for processing to take place. It is also critical that any new uses are determined by “data controllers” only, and not any organisation that is classed as a “data processor”. If individuals could not be judged to have foreseen this new use, then their consent to process for that new purpose must be sought afresh.

Of course legislation may allow such a new use, and in this instance legal counsel should be consulted as to the correct legal way forward.
All involved parties must be aware of how their own privacy notices are worded and how such wording may restrict or open up different uses for personal data. Any changes to the usage of LRS data must be communicated by LRS back to the group members so the privacy notices can be altered to reflect the changes.

5. Learner types

There are some learners who require to be identified and measures taken to ensure their details are secure, beyond the tight security measures already in place.

5.1. Vulnerable learners

Learners that are classed as vulnerable may include domestic violence victims, protected persons, those with learning difficulties or those who have officially appointed representatives or guardians.

A wide range of social contexts may arise that mean that the LRS may be asked to take additional steps to protect the privacy of a specified individual. The LRS will generally consider these circumstances on the advice of the organisation representing the individual or in line with any concerns raised by the learner.

5.2. VIPs and others in the public eye

These learners include members of the royal family, senior public figures and others, whose identification and disclosure of personal details may present a security risk to them, the wider public, or the nation.

5.3. Offenders

Learners who are offenders or who are in detention, or whose learning provider is/was technically a place of criminal detention are entitled to protection from disclosure of their location and their offender status.

Skills Funding Agency

6. Requests for information under law

Requests for information from the LRS will usually fall under two pieces of legislation. Initially a request for information of any government department is made under the Freedom of Information Act 2000. If the request is deemed to be a request for personal information, made by the person themselves or a recognised representative of that person, then the request will be dealt with via the Data Protection Act 1998.

6.1. Freedom of Information Act 2000

The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 give everyone the right to ask for information held by a public authority, to be told whether the information is held, and unless exempt, to have a copy of this information.
The Freedom of Information Act applies to public authorities. It also applies to companies which are wholly owned by public authorities. Organisations are required by law to provide the information requested or explain why the information is being withheld within 20 working days of the receipt of a written request.
The Act also requires public authorities to have an approved publication scheme, which is a means of providing access to information that an authority proactively publishes and which is readily available to those that wish to access it.
The Skills Funding Agency will handle these requests in accordance with their policy for handling FOI requests.

6.2. Data Protection Act – Subject Access Request

Requests for personal data, made by the individual themselves or an authorised representative of the individual are called Subject Access Requests (SARs).
This determines that on receiving a SAR, in writing, a Data Controller must supply the information requested or explain why the information cannot be supplied by way of an exemption within 40 calendar days from receipt of the request.
Personal data about any persons other than the applicant will generally be exempt from disclosure and redaction or refusal of such information will take place.
SARs will be handled by the Skills Funding Agency and more information on requesting the personal information that is held by the LRS and PLR and more widely the Skills Funding Agency can be found at www.skillsfundingagency.bis.gov.uk. You will need to provide your name, address and other details to enable us to locate your information on our systems. You have a right to have any codes or technical language that relates to your information explained to you.

Skills Funding Agency

7. Use of legal powers

Amongst the LRS partners there are several pieces of legislation that have a day to day impact on the sharing of personal data, the main one of these being the DPA. However, other laws exist that may have provision for the sharing of data with other organisations, irrespective of the DPA. One of these Acts is the Finance Act and parts of this legislation permit, for example, the HMRC Inland Revenue to access some personal data from some partners for specific purposes.

Due to the number of departments that partners may deal with and the number of Acts under which provision might be given for access to shared data, it is not practical to try and identify all such legal gateways in this framework.

Partners should be fully aware of the Acts under which they operate both in terms of acquiring personal information and providing personal information. Considering access to personal information should be part of a process within any organisation where requests are considered in their own merits and an audit trail of information flows recorded, to support the sharing decisions made.

8. Data quality

The fourth principle of the Data Protection Act 1998 states that "*Personal data shall be accurate and, where necessary, kept up to date*".

The LRS has implemented a Data Quality Strategy. The strategy will ensure a defined and proactive approach to data quality.

The LRS will influence data quality through:

- Data Standards e.g. Common Data Definitions – This will improve the interoperability of the data between the LRS and stakeholder organisations reducing the amount of records being mismatched or corrupted.
- Business/Validation Rules – Implementing business/validation rules at the system level will constrain the data loaded into the PLR allowing the LRS to validate records and reject non-conforming records.
- Data Quality Reporting – The LRS will offer a suite of pre-defined reports to assess the quality of the data in the PLR system. This extensible list of reports will form part of the Data Quality Strategy.
- Stakeholder Quality Assessment – Stakeholders will receive ad-hoc feedback regarding data quality and furthermore will be encouraged to implement data quality checking routines before data is sent to the LRS. This two-way process is essential in partnership working to improve data quality.
- Data Quality Audit(s) – Periodic Data Quality Audits to assess the LRS's approach to data quality and to review derived metrics around data quality.

The LRS Data Quality Framework will be embedded into relevant LRS business units ensuring data quality is embedded in business as usual (service and data management) processes with data quality analysis management information reports created and available to senior management as required.

The benefits of the data held within the LRS and shared on an ongoing basis will be dependent on quality and timeliness. With regards to participation and achievement data the LRS will endeavour to optimise the balance between timeliness and quality.

All proposed future achievement and participation data will be assessed for quality and timeliness through the use of user groups and the LRS undertaking data analysis.

9. Data challenge and correction

The LRS offers learners and organisations a process and system for challenging and correcting data.

LRS data challenge is the process which allows an individual, a Learner Registration Body (LRB) or Helpdesk to address problems with the Personal Learning Record details. The PLR is composed of the Learner registration details and relevant achievement & participation records. The LRS will act as a conduit for addressing data problems with the Personal Learning Record.

The basic stages of the data challenge (DC) process are:

- Raising a data challenge (Online, via LRB or via helpdesk)
- Processing a data challenge

- Closing the data challenge

Data challenges are raised and must be routed to the appropriate authorising source. An authorising source is the organisation who is responsible for deciding if the data challenge is correct (or not) and deciding who will authorise any necessary changes. Where changes cannot be actioned by the authoritative source the LRS Data Challenge team will be responsible for ensuring the change is applied in relevant systems.

Learners may obtain data challenge status updates either online, by contacting the helpdesk or via a learner registration body.

10. Information and data security

The seventh principle of the DPA states that "*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*"

The personal and sensitive personal data held about individuals will be controlled carefully as part of a comprehensive Information Governance framework.
It is an individual organisation's responsibility to ensure that any confidential information held is secure, both in terms of electronic security, physical security and process security.
The International Standards Organisation ISO27001: "The International Standard for an Information Security Management System", is a practical way for many organisations to ensure that their processes, policies, security and management of information are as robust as possible. All security arrangements put in place should use this or the equivalent standard as a guide and it is expected that LRS partners have in place IT security and management policies commensurate with the types of data they process and share. LRS controls in this area are detailed below.

10.1. The Learning Records Service Information Security

The LRS is actively committed to ensuring that the appropriate security, integrity, availability and confidentiality of LRS and LRS stakeholders' information are preserved.
The LRS has implemented an approved Security Policy to protect its assets from all threats whether internal or external, deliberate or accidental.
It is a policy to ensure that:

- ***Confidentiality*** of information is assured
- ***Integrity*** of information is preserved
- ***Availability*** of IT Systems is maintained
- ***Regulatory*** and ***legislative*** requirements are met
- ***Business Continuity Plans*** are produced, maintained and exercised
- ***All breaches of security***, actual or suspected are reported up the Management chain, and investigated by the **Security Manager**
- ***Advice and Guidance*** on Information Security is available to all staff

- The LRS has implemented standards and processes, where necessary, to support the implementation of this policy.

The LRS Security Policy complies with the requirements of ISO27001: The International Standard for an Information Security Management Systems and has been developed as a Summary of Controls (SoC) in accordance with the ISO standard; it incorporate ISO Standard requirements.

The LRS Security Policy will be accredited by the Skills Funding Agency to ensure the policy is upheld and documented in the Risk Management Accreditation and Documentation Set.
The Skills Funding Agency's Information Security Policy has been consulted in the creation of the LRS policy document.
The LRS Security Manager has direct responsibility for maintaining this policy, and is further responsible for providing advice and guidance on its implementation.
All managers are directly responsible for implementing this Security Policy within their business areas, and for ensuring adherence to the Policy. It is the responsibility of each member of staff to adhere to the Learning Records Service Security Policy.
The Security Manager maintains a Risk Management System which contains details of a wide range of potential security threats, risk ratings (based on consultation with stakeholder groups) and security measures which have been implemented to guard against security breaches. All risks are rated and linked to owners as well as to the relevant mitigating action.
The Risk Management System has been chosen for consistency with other agencies in the education sector, and the log and measures are regularly reviewed and updated to address emerging threats, as well as ongoing developments to the LRS service;
Security measures implemented by the LRS cover four areas:

- Technical – e.g. firewall, virus protection, and data transfer procedures etc.
- Procedural – e.g. through the Organisation Agreement, help desk procedures etc.
- Physical – Premises access control and security, guarding of data centre.
- Personnel measures – e.g. training and appropriate vetting and clearances of personnel.

The technical architecture is based on Linux servers which reduces threats, such as viruses and Trojans, which are malicious pieces of software that can harm computers and the data that they hold.
LRS data is held on a server within a secure data centre located in the United Kingdom.
Personal Data is not transferred overseas and any development work done outside the United Kingdom uses dummy data.
There is a full annual audit and additional audits are conducted when required.
The role of all personnel in ensuring security is emphasised.
Penetration testing is undertaken on all system developments prior to release.

Incident control measures are in place to cover emergency events.
Procedures are in place to monitor unusual behaviour such as the creation of unexpected numbers of users.

10.2. Staff Training

Any organisation dealing with personal and sensitive data has a duty to ensure that all relevant personnel are advised of, and understand, the implications of the Data Protection Act 1998, and any other legislation which the organisation might be subject to.

It is considered that it is an individual organisation's responsibility to ensure that all relevant staff are correctly trained and informed, in the handling of personal and sensitive personal data.

It is also recommended that each organisation, if they have not already done so, appoint a person or people who will be responsible for ensuring that data sharing and data protection issues are addressed within their organisation promptly and correctly, and represents, where applicable, the organisation with regard to data sharing issues. This may be a permanent member of staff or a third party contractor/consultant specialising in this area.

In certain circumstances it is advisable that staff that have access to the personal information of young people are checked with the Criminal Records Bureau (CRB). Consideration should however, be given to whether or not the role falls within the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 as amended.

10.3. External Consultants/Contractors

Organisations may use contractors or consultants who may in turn have access to any personal or sensitive personal data held by the organisation they are working for. If a consultant/contractor is expected to, or actually does, transfer data from the organisation they are working for, to their own computer system for processing or storage, it is expected, under the terms of this framework and under the regulations of the Data Protection Act 1998, that the consultant/contactor will have a suitable agreement in place that determines the consultant/contractor as a data processor, or an individual accessing data under the controllership of their client.

Such an agreement must be explicit in stating the requirements placed on the consultant/contractor in terms of the use of the data, security of data that they may take off-site and the fact that they will use the data according to the principles of the DPA.

It is strongly recommended that the contractor\consultant becomes data protection registered with the ICO for the purposes of handling LRS Information.

11. Retention & Disposal of Data

The fifth data protection principle states that "*Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes*".

All organisations will have in place a retention and disposal schedule preferably forming part of a comprehensive records management strategy. This schedule should identify the types of data held and used by the organisation and list the retention and destruction requirements for these data.

11.1. Retention of Data

Shared data will be used for differing purposes amongst LRS partners and consequently retention times for these data will vary. It is important however, that any retention requirements either via guidelines or published in law are adhered to.

Part of the rationale for the creation of the service was the creation of a life long record of learning. As such, it was originally envisaged that the ULN, Learner Registration Details and Personal Learning Record should be kept for a period of 66 years, to allow the system to cope with extremes where, for example, a learner does not have new learning outcomes from age 16, but "reactivates" the system in their 70's as they undertake relevant training or education again. This LRS intends:

- to allow individual options the right to have Personal Learning Record information disassociated from their personal details once they are no longer in the education system
- to provide a "sunset process" for records which are not used for an extended period (66 years).

Data sharing between LRS partners and third parties will have retention periods defined, depending on the use to which the data will be put.

11.2. Destruction of Data

Once shared data are finished with and the purposes that the data have been shared for has been fulfilled, the organisation will convert the data to aggregated form, for long term statistical storage if required, and/or delete the now redundant individualised data from their systems.

The LRS will have the right to request that this is done in accordance with any data sharing agreements in place, and if necessary request audit proof that this has taken place.

The deletion of data includes paper versions/hard copies. All records of any format should be regarded as confidential waste, and be discarded appropriately.
The destruction of data passed to the LRS via removable media will be monitored through the LRS Data Destruction register. The LRS will destroy all data transferred by CD\DVD media through the use of a purpose build CD destruction mechanism.

11.3. Audit Control

Organisations that provide or receive personal and sensitive data from the LRS must have in place processes that ensure that any data processed, moved or deleted can be retrospectively tracked, in the form of audit trails. Database systems often provide transaction and audit logs and it is important that these processes are in place in case an instance arises where the movement of data needs to be audited in future.

Another area of audit control is to ensure that version control is in place. This is especially important for organisations that have constantly changing databases/datasets and data should be able to be tracked back to specific versions of the datasets as required.
Individual organisations should have these processes in place, and partners who are sharing information should satisfy themselves that their data sharing is taking place with an organisation that has the necessary security and audit policies in place.

11.4. Exceptions to the Data Protection Act

On occasion it may be necessary for an organisation to disclose personal and sensitive personal data without the consent of the individual.
These instances may be for crime prevention or detection or when required by law.
On these occasions full cooperation with the requesting organisations is expected by the organisation concerned, subject to their own legal guidance. However data should only be provided on this basis, when it is proven that there is a relevant right of access to personal data.

12. Data sharing process and agreement

As a document under periodic review, this framework may be subject to change either through agreement with LRS partners, or through changes in legislation.
If changes are required, a new version of this document will be issued and published in accordance with the Skills Funding Agency publishing scheme.
This framework agreement serves to provide detailed information to the learners and the public about LRS PLR data sharing and also the requirements expected of organisations involved in using the information provided from these systems.
Any future review of the Framework Code of Practice for Sharing Personal Information will consider the following:

- The sharing of information is having the desired effect
- Privacy notices still provide an accurate explanation of your information sharing activity

- Procedures for ensuring the quality of information are being adhered to and are working in practice
- Organisations sharing information are meeting agreed quality standards.
- Retention periods are being adhered to and continue to reflect business needs
- Security remains adequate and, if not, whether any security breaches have been investigated and acted upon
- Individuals are being given access to all the information they are entitled to, and that they are finding it easy to exercise their right.

Skills Funding Agency

Appendix A – Bodies with whom the Learning Records Service Shares data with

Any information shared must be done in accordance with the principles of the Data Protection Act 1998, and be fully justified with respect to the individual. This list is heavily based upon section 537a prescribed regulations for England. For devolved administrations we will agree specific list in line with relevant statutory Instruments and legislation applying to those administrations.

The management committee of a pupil referral unit at which the relevant pupil is or was registered.	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
The Training and Development Agency	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
The States of Guernsey Education Department	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.

Skills Funding Agency

The States of Jersey Education Department	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
The Isle of Man Department of Education	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Welsh Assembly Government	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties and subject to appropriate legislation.

WJEC CBAC Limited	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Student Loans Company	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Universities and Colleges Admissions Service (UCAS)	LRS shares data with UCAS under the pre-condition of a signed Organisation Agreement and where relevant a completed LRS Standard Data Sharing Agreement with Third Parties to enable UCAS to verify qualification data.
Higher Education Statistics Agency (HESA)	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
University for Industry (UFI) Ltd	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Any person with whom a relevant local authority has made arrangements under section 68 or section 70 of the Education and Skills Act 2008	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.

Any person, who, either alone or jointly with others, awards or authenticates any qualification accredited by the regulatory body.	LRS shares personal data for the purposes of enabling 14-19 diplomas and other QCF qualifications. Currently any organisations wishing to access this data must either have signed the Organisation Agreement or completed the LRS Standard Data Sharing Agreement with Third Parties.
The Skills Funding Agency	LRS shares personal data for the purposes of enabling 14-19 diplomas and other QCF qualifications. Currently any organisations wishing to access this data must either have signed the Organisation Agreement or

	Completed the LRS Standard Data Sharing Agreement with Third Parties.
The Qualifications and Curriculum Development Authority (QCDA)	LRS shares personal data for the purposes of enabling 14-19 diplomas and other qualifications to be awarded to the learner. The QCDA sign an Organisation Agreement.
Institutions and Providers within the Further Education sector	LRS shares Personal data where the organisation has registered with LRS as a Learner Registration Body and signed the Organisation Agreement.
Primary Care Trusts	LRS may share data with these organisations upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Work-based learning providers	LRS shares Personal data where the institution has registered with LRS as a Learner Registration Body and signed the Organisation Agreement.
Approved UK research institutions.	LRS may share data with such persons upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.

Learning providers registered with the LRS UK Register of Learning Providers (UKRLP)	LRS may share data with these organisations upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Institutions within the higher education sector (HEIs)	LRS may share data with such organisations upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties.
Northern Ireland Assembly	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties and subject to appropriate legislation.

Scottish Government	LRS may share data with this organisation upon acceptance of a completed LRS Standard Data Sharing Agreement with Third Parties and subject to appropriate legislation.

Skills Funding Agency

Appendix B – Relevant legislation & useful contacts

As summarised in the introduction to this document, the following pieces of legislation have been considered when creating this data sharing framework. Links to online texts of the legislation have been provided, where applicable.

Data Protection Act 1998

This is the key piece of legislation that affects any data sharing that may take place.
http://www.legislation.gov.uk/all?title=data%20protection%20act%201998

Human Rights Act 1998

Available from http://www.legislation.gov.uk/all?title=human%20rights%20act

Disability Discrimination Act 1995

As amended by the Special Educational needs and Disability Act 2001
Available from
www.legislation.hmso.gov.uk/acts/acts1995/Ukpga_19950050_en_1.htm

Freedom of Information Act 2000

Available from
http://www.legislation.gov.uk/all?title=freedom%20of%20information%20act%202000

Other Useful Contacts

Information Commissioner's Office including register of data controllers – https://ico.org.uk/
British Standards (BS7799/ISO27001) – www.bsi-global.com
Learning Records Service – www.learningrecordsservice.org.uk

Skills Funding Agency – www.skillsfundingagency.bis.gov.uk

Department for Education – www.education.gov.uk
Learning Provider Register – www.ukrlp.co.uk
Information Standards Board - http://data.gov.uk/education-standards/