

Data Protection, Lifelong Learner Record Systems & ePortfolios: A Short FAQ

Andrew Charlesworth and Anna Home - Centre for IT & Law, University of Bristol
Researchers, JISC Study to explore the legal and records management issues
relating to the concept of the Lifelong Learner Record

Q: Data protection is a concern of ours, but if the only personal data about learners we wish to add to our LLR/ePortfolio system is personal data that we already hold in institutional systems, then are we automatically in compliance with the law?

A: Under the Data Protection Act 1998, an institution that determines the purposes for which and the manner in which any personal data are, or are to be, processed is a 'data controller'. Data controllers have a number of obligations under the Act with regard to 'data subjects' whose personal data is processed. An institution will usually have notified the Information Commission of the purposes for which it intends to process personal data - it is important to ensure that this institutional notification does in fact cover the intended operational uses of the ePortfolio system. It should not simply be assumed that the notification is adequate for that purpose, or that the institutional data protection officer is automatically going to be aware of the likely uses of the ePortfolio system. This is particularly important if there is any intention to permit the transfer of personal data from the ePortfolio system to 3rd parties.

Data controllers are required by the Act to process personal data only where they have a clear purpose for doing so, and then only as necessitated by that purpose. A data controller's purpose for any personal data processing operation should thus be clearly set out in advance of the processing, and should be readily demonstrable to data subjects. To that end, the Act requires data controllers to provide data subjects with a basic minimum amount of information about the collection, use, and distribution of their personal data. Most institutions provide this information to data subjects by means of collection notices at the point when the personal data is collected. However, if existing collections of personal data are to be imported into an ePortfolio system and in particular where this permits different uses, and allows access to the data by different third parties, than those already identified to the data subjects, then information about those uses by, and transfers to and from, the new system should be provided to data subjects.

Data held in the ePortfolio system must be held in accordance with the Data Protection Principles <<http://www.hms.gov.uk/acts/acts1998/80029--1.htm#sch1>>. All new institutional administrative systems utilising personal data should be audited for compliance with the principles before 'live data' is used; and regular checks should be carried out to ensure continuing compliance of both the system and associated administrative procedures. Provision for initial and continuing compliance audits should be made when considering long term budgeting for such a system.

Q: How, and when, should we deal with data protection compliance issues?

A: When developing an ePortfolio system, ensuring compliance with data protection law should always be built into the planning/design process. Proposed uses of personal data, as well as potential 3rd parties from whom transfers of personal data may be received into the system, or to whom data may be transferred from the system, should be identified and their respective data protection risks identified and the institutional responses documented. Institutional data protection officers should always be involved in this process. When the system is operational

the institution must take such steps as are necessary to ensure that it is able to demonstrate continued compliance with its obligations under the Data Protection Act 1998. Data subjects, institutional employees and 3rd parties permitted to access the personal data should all be regularly reminded of their rights and obligations as regards the system. All proposed future changes to the system, both technical and administrative, should be reviewed for their data protection implications prior to their implementation, and where necessary, advice on their impact should be sought from institutional data protection officers, or the Information Commissioner.

Q: Our ePortfolio system will be part of a multi-institutional system and the personal data we collect from our students will be processed on our behalf by another institution. How does this affect our data protection obligations?

A: In circumstances where there may be multiple data controllers using the system it is a useful exercise to map the potential personal data flows within the system, in order to identify where particular data protection responsibilities and obligations will lie. Remember that a data controller is an institution that determines the purposes for which and the manner in which any personal data are, or are to be, processed. An institution that processes personal data on behalf of a data controller, and does not determine the purposes for which, and the manner in which, any personal data are, or are to be, processed, is not a data controller, but a 'data processor'. A data processor has no statutory obligations under the Data Protection Act 1998, as regards processing it carries out on behalf of the data controller. The Act places the burden for ensuring that data processors do not breach its requirements upon the data controllers who use them. Because of this, data controllers need to ensure that their relationship with a data processor is governed by a formal data processing agreement which clearly outlines the contractual relationship between data controller and data processor, requires the data processor to process in conformity with the Act, and provides the data controller with suitable access to audit the data processor's compliance with the terms of the agreement.

Data controllers who share personal data on data subjects for different purposes are referred to as 'data controllers in common'. In this case, each data controller remains individually responsible for the processing they have carried out on the personal data. Data controllers who share personal data on data subjects for the same purpose are referred to as 'joint data controllers'. Joint data controllers are jointly liable for any breach under the Act. Where an ePortfolio system is mapped in advance of its introduction, such relationships between the parties can be more readily identified.

Q: If joint data controllers are jointly liable for any breach under the Data Protection Act 1998, how can data controllers who are compliant with Act protect themselves from the acts and omissions of their fellow joint data controllers?

A: Where a number of data controllers are acting as joint data controllers for a particular purpose, they would normally enter into a Data Controller Agreement. A Data Controller Agreement is a contract between two or more institutions that sets out the terms and conditions under which each institution may process the jointly-held personal data. In most circumstances, parties to a data sharing agreement will have notified the Information Commissioner that they wish to be registered as Data Controllers and, as such, one requirement of membership of an Agreement may be the production of the Information Commissioner's notification number. The Data Controller Agreement will usually contain:

- undertakings by the parties as to the extent of their obligations under the Agreement.

- warranties by the parties about their compliance with the Act, and the appropriateness of their technical and procedural security
- indemnities by the parties designed to ensure that failures on the part of one party to the agreement will not unduly penalise the other joint data controllers.

An Agreement should make provision for parties wishing to withdraw from it, and for termination of the whole Agreement. It should also deal with issues such as procedure for communications between parties, and jurisdiction and choice of law in the event of disputes between the parties.

Q: OK, we would like to undertake a data protection mapping exercise for our project. How might we do this?

A: This type of exercise can be carried out in a number of ways, and the most effective way will largely depend upon the size and scope of the project to be mapped. The method outlined below has been used by the authors to map a distributed multi-institutional LLR project linking a range of educational service providers, a data processor and a range of third parties. See <<http://www.tuc.org.uk/extras/UEODataFlows.pdf>>.

Step 1 Identifying the data protection actors

The initial task is to determine who will be providing, obtaining, recording or holding personal data or carrying out any operation or set of operations on personal data within the project; or will receive personal data for those purposes from the project or its partners.

For example, in this simple hypothetical:

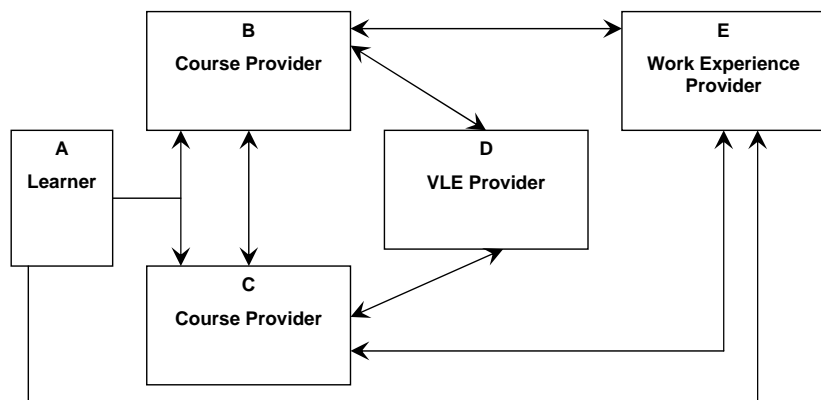


Fig. 1 NB - Personal data flows back to the learner as the Data Subject are not indicated in this diagram.

Here the learner (A) is taking a course jointly provided by 2 institutions (B & C) which is delivered by means of a VLE provided by another organisation (D). Part of A's course involves a work placement with a Work Experience provider (E). The arrows indicate likely transfers of learner personal data, and the direction of those transfers.

When identifying actors, it is worth considering the implications of proposed or potential future expansion of a project, both in terms of adding to existing types of actor, as well as including new types of actor. This may help in planning for future scalability, and also

influence the nature of the contractual and administrative frameworks that are adopted. Recent developments aimed at increasing interoperability of institutional LLR/ePortfolio systems at a regional, and possibly national, level should not be overlooked.

Step 2 Identifying proposed purposes for data transfers and processing

In order for processing of personal data to be lawful, it must be carried out for a specified purpose or purposes and that purpose or purposes must normally be disclosed. Once data is collected for a specific purpose or purposes it may not be used for other secondary and undisclosed purposes. In our hypothetical, B & C collect personal data from A for the purposes of providing A with an educational service, and to permit themselves to carry out necessary administrative functions, including learner registration & certification, statistical reporting administration of courses, providing special needs support, obtaining appropriate funding from funding bodies etc. D is provided with limited personal data about A from B & C in order to provide certain VLE services and may provide personal data about A back to B & C e.g. VLE usage statistics. E will be provided with personal data directly from A, e.g. information required for health and safety; and personal data about A from B & C as part of the administration of the work experience process. In turn, B & C will receive personal data about A from E concerning A's performance on work experience.

Step 3 Determining data protection roles

Having determined who the data protection actors are within a scenario, it is then necessary to work out what their roles are. In this hypothetical, A is the data subject, as they are the subject of the personal data being processed/transferred. B & C are processing A's data for the same purpose (the provision of A's course) and are thus joint data controllers for that data. D is processing A's data on behalf of B & C and is not determining the purpose and manner in which A's data is processed. D is thus a data processor. E is using data from A, B & C and providing data to B & C. It is likely that E is the data controller for the data obtained from A, and, depending on the purposes to which the data obtained from B & C is put, that E is either a joint data controller with B & C, or a data controller in common.

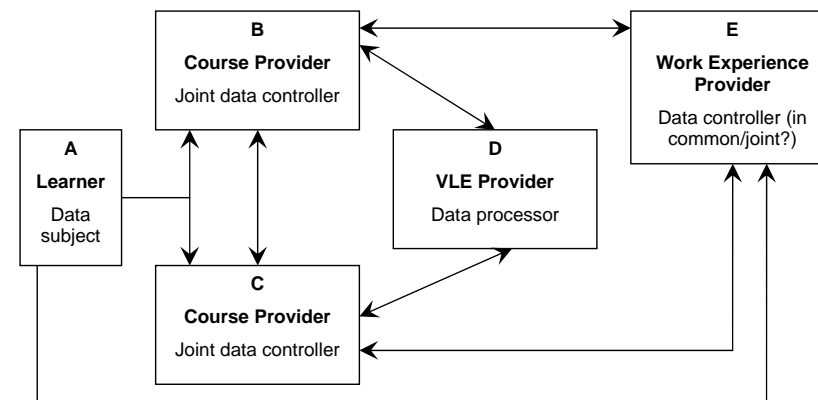


Fig. 1 NB - Personal data flows back to the learner as the Data Subject are not indicated in this diagram.

Step 4 Considering categories of personal data to be processed/transferred

Once data protection actors and roles have been identified, it is necessary to consider the categories of personal data that will be needed to be processed/transferred, in order to adequately fulfil the proposed purposes. Under the Act, data processed for a particular purpose must be adequate, relevant and not excessive in relation to that purpose. For example, B & C may collect a wide range of personal data from A to meet their proposed purposes (name, address, contact details, educational records, special needs requirements) but they should not collect information simply because they think it might be interesting or useful at some later point, if they lack a purpose for processing it at the time of collection. They may also not use data legitimately collected for one purpose, for another undisclosed purpose, e.g. if special needs information is collected for the sole stated purpose of ensuring adequate service provision, it may not then be used for the purpose of determining admission to a course of study.

Step 5 Identifying personal data that is 'sensitive personal data'

Once the categories of personal data that are adequate, relevant and not excessive to the purposes for which it is proposed to process them have been decided, it is necessary to consider whether any of them are 'sensitive personal data'. The Act defines sensitive personal data as personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences. Thus any category of personal data that it is proposed to collect which falls within, or is likely to implicate, one of those headings will require special consideration. In the hypothetical for example, it is possible that B & C, as course providers, may require special needs information from A for the purpose of ensuring adequate service provision. Such information will be personal data relating to physical or mental health and will thus be sensitive personal data.

Step 6 Determining which processing conditions might justify the processing/transfer

Schedule 2 of the Act lists a number of specific conditions for all processing of personal data and Schedule 3 of the Act lists a number of specific conditions for the processing of "sensitive" personal data.

- For "ordinary" personal data, at least one of the conditions of processing must be met before the processing can take place. The conditions are:
 - the individual has consented to the processing
 - processing is necessary for the performance of a contract with the individual
 - processing is required under a legal obligation (other than a contractual one)
 - processing is necessary to protect the vital interests of the individual
 - processing is necessary to carry out public functions, e.g. administration of justice
 - processing is necessary in order to pursue the legitimate interests of the data controller or third parties and does not unjustifiably prejudice the interests of the individual
- For "sensitive" personal data, one of the ordinary processing conditions and one of the conditions for processing sensitive data must be met before processing can be carried out. The conditions for processing sensitive data are that the data subject has given his or her explicit consent to the processing of the personal data, or that the processing is necessary for a further set of specified reasons, including

- It is required by law for employment purposes
- It is needed in order to protect the vital interests of the individual or another person
- It is needed in connection with the administration of justice or legal proceedings

It is possible that the purpose for which a data controller requires the information could be capable of justification under a number of the conditions. It is useful at an early stage to determine which condition is to be relied upon.

Step 7 Choosing processing conditions

It can be seen that consent of the data subject appears in both the Schedule 2 and Schedule 3 list of conditions. It may thus be tempting for institutions to simply request consent for all proposed uses of a data subject's personal data. However, it is worth noting some points about consent.

- if a data subject's consent is to be relied on to provide a Schedule 2 criterion for lawful processing, then the fact of consent cannot be simply assumed by a data controller (e.g. where a data controller sends out a form stating that in the absence of a negative response from a data subject their consent will be assumed).
- Where there is obvious inequality of bargaining power between the data controller and data subject, it may also be difficult to demonstrate the 'freely given' element of consent.
- Consent may be withdrawn by the data subject at any point, a fact that may prove problematic for data controllers where consents are obtained for data processing purposes without which the data controller cannot provide an essential service - in other words where the learner's consent cannot be withdrawn without in effect ending the learner's involvement in the institution.

In the hypothetical, A's course involves the transfer of limited personal data from B & C to D, the VLE provider, for the purpose of VLE administration. B & C could ask for A's consent to this transfer, but, in practice it would probably be more efficient to rely upon the criterion that the processing is necessary for the performance of a contract between A and B & C (e.g. the contract for the supply of an educational service). However, as regards the processing of sensitive personal data, the options are rather more restricted, and in most cases explicit consent is likely to be the most effective, or indeed only, option.

Step 8 Dealing with the issue of data subject consent

Where consent is to be the criterion under which processing of particular personal data is to be justified, it is necessary to consider where in the process that consent can be most effectively obtained. It may be that consent would be best obtained at more than one point in the process, e.g. if personal data is collected from A, as part of the registration process for the course, and consent is deemed to be required for the processing of that information, then clearly it makes sense for B and/or C to obtain that consent, as they will be the joint data controllers, and will thus be in the best position to react to a withdrawal of consent by A at a later stage. However, as regards personal data required by E, it may be that consent will be required from A for different personal data that that which was initially required by B & C. In this case, consent might best be obtained by E, as E may be in a better position than B & C to react to withdrawal of consent by A for that particular data.

Step 9 Determining when collection notices should be provided to data subjects

A collection notice is used by a data controller to provide a data subject with information relevant to the processing of their personal data, at the time of its collection. It will describe the purposes for which the data controller intends to process their personal data, and should also include details of joint data controllership, as well as indications of third parties to whom the data may be disclosed or transferred, and the purposes served by those transfers or disclosures. As such, the collection notice does not need to cover every specific eventuality, but must provide sufficient information to demonstrate that a data subject could have 'reasonably expected' their data to be processed in the manner the data controller intends. The collection notice should provide enough information to the Data Subject to allow them to utilise effectively the rights provided to them by the DPA 1998 (e.g. subject access).

Because collection notices are vital to the effective utilisation of the Act by data subjects, it is important to consider where and when in the process they should be made available; how, and by whom, will provision be made for data subjects to re-access collection notices at a later date; how, and by whom, will changes to a collection notice be notified to relevant data subjects?

Step 10 Dealing with the issue of data subject access

Subject access means that a data subject is entitled to be told by a data controller whether personal data about them is being processed by, or on behalf of, that data controller. Subject access requests (SARs) can only be made to data controllers, and not to data processors. In the hypothetical, therefore, a SAR can be made by A to B, C and E, but not to D.

If the data controller is processing personal data about a data subject, the data subject is entitled to a description of that personal data. They are also entitled to know the purposes for which the personal data are being, or are to be, processed, and to be informed about the recipients, or classes of recipients, to whom their personal data have been, or may be, disclosed. Data subjects are also entitled to a copy of their personal data in comprehensible form, as well as any information held by the data controller as to the source of those data.

The issue of whether E is a joint data controller with B & C is also relevant here. If they are joint data controllers of personal data about A and they hold no personal data on A as sole data controllers, a SAR made to any of them by A should reveal all the personal data they jointly hold.

However, if E is a data controller in common, then a SAR made by A to B & C will not reveal the personal data about A held by E, but should identify that B & C have passed personal data about A to, and received personal data about A from, E. A will have to make a separate SAR to E to discover the extent of E's personal data holdings on them.

If E holds some personal data about A jointly with B & C, but also some personal data about A which has not been disclosed to B & C, then a SAR made by A to B & C will reveal the jointly held data but not the data held solely by E, conversely a SAR made by A to E should result in the disclosure of both the jointly held and solely held information.

In such circumstances, it is good practice for the parties acting as data controllers to provide clear indications to data subjects as to their respective relationships, and the appropriate avenues for submitting SARs. As the effective exercise of many subsequent rights (e.g. the rights of correction and erasure) depend upon the data subject obtaining this information, it is critical that the subject access mechanism implemented by data controllers operates in an efficient and timely fashion. To this end, it is essential that, in systems, the roles of the relevant institutions are clearly understood (who is a data controller, who is a data processor

etc.), and that the responsibility for providing effective subject access to data subjects to their personal data, at all points in the process, is clearly delineated.

Step 11 Plotting necessary contractual agreements between data protection actors

Once the basic mapping is carried out, it should be possible to determine the necessary contractual agreements that will be required between the various data protection actors. For example, in the hypothetical, it appears that B & C (and possibly E) are likely to need a joint Data Controllers Agreement. B & C are also each going to want to have a Data Processor Agreement with D. If E is not a joint data controller with B & C, then B & C may also want to have a formal Data Sharing Agreement with E outlining the conditions under which they are prepared to transfer learner personal data about A.

Step 12 Considering necessary administrative documentation

At this stage it should be possible to start considering the administrative documentation required for the data protection process. This may, for example mean:

- including within the project Service Definition a section defining the personal data required for the purposes of the project
- developing a Data Controller Protocol which outlines the necessary conditions with which any Data Controller must comply before being eligible to enter into the project Data Controller Agreement. This will detail the types of measures required to meet the terms and conditions of the Data Controller Agreement, for example a condition that requires member institutions to have 'appropriate technical and procedural security'. This will allow the current and prospective members of a Data Controller Agreement to adhere to a consistent set of measures, which are capable of change over time without requiring continual changes to the Data Controller Agreement, e.g. when new technologies require alterations to what is commonly understood by 'appropriate technical and procedural security'.
- examining the notifications made by the parties to the project to the Information Commissioner to ensure that they all accurately reflect the processing to be carried out by the project
- drafting necessary consent forms, collection notices, and information documents e.g. about appropriate avenues for submission of SARs
- drafting a document outlining the data protection mapping process, listing the reasons for project decisions about purposes of processing; rationales for requiring categories of data; reasons for assignment of actor roles; decisions about data sensitivity; rationales for the use of Schedule 2 & 3 criteria to justify particular processing; reasons for timing of obtaining of consent and provision of collection notices; and decisions as to how subject access requests will be handled within the project

Step 13 Plotting the necessary institutional infrastructures

Mapping the data protection process will also permit a project to start developing a suitable administrative framework to ensure that processes such as provision of collection notices, collection of consent, and handling of SARs are dealt with efficiently. Without an effective administrative framework, much of the value of the data protection mapping will be lost. As institutional responsibilities are mapped, it is possible to allocate tasks within institutions and projects, and to conduct meaningful cost/benefit and risk analyses for each. This will enable a

clearer picture of the potential costs, and permit projects and institutions to make staffing and budgetary allocations accordingly.

Step 14 Identifying probable information dissemination and training needs

Finally, the mapping process should provide a clearer picture of areas of institutional/project activity where data protection information and/or training will be required for staff, and the nature of that training. Adequate staff training, and the ready availability of information about project and institutional data protection processes, will be vital to a project meeting the compliance requirements of the data protection legislation.

Q: This is all a little overwhelming, are there any other sources of information that I can read on data protection?

A: There are a range of publications dealing with the Data Protection Act 1998, for example:

Peter Carey (2004), *Data Protection: A Practical Guide to UK and EU Law*, Oxford University Press, ISBN: 0199265682, £49.95

Rosemary Jay (2003), *Data Protection: Law and Practice*, Sweet & Maxwell, ISBN: 0421794801, £172.00

There are also a range of webpages which deal with the issues more generally, for example:

JISC Legal Briefing Paper - Data Protection

<<http://www.jisclegal.ac.uk/dataprotection/dataprotection2005.htm>>

Information Commissioner's Office, Factsheet: What is the Data Protection Act (DPA)?

<<http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%20Fact%20V2.pdf>>

This document is a work in progress. If you would like to see this FAQ cover other areas of law, address existing areas in more detail, or answer specific questions, or indeed if you would like to contribute to it, please contact the researchers at:

Email: <A.J.Charlesworth@bris.ac.uk> or <Anna.Home@bristol.ac.uk>

Address: The Law School, University of Bristol, Wills Memorial Building, Queens Road, Bristol BS8 1RJ

New discussion list: EPORT-LEGAL@jiscmail.ac.uk

See <<http://www.jiscmail.ac.uk/lists/EPORT-LEGAL.html>>