Electronic Verification Information Pack

Disabled Students Allowances


SLC
Student Loans Company

Version Control

Created Date	Revision Date	Author	Version No.	Details/Comments
27/03/2014	30/12/2014	Vicki Riley	0.3	Email contacts updated throughout Update to submission requirements – additional information included regarding submission route for email verification Text added to administrator verification request
	14/01/2015	Jonathan Oakley	0.4	Updated path to live.
	06/01/2017	Matthew Ferris	0.5	Removed standard information required on supporting documents bookmark.
	20/05/2022	Matthew Hall	0.6	Data Protection section amended to reference UK GDPR.

Contents

Overview

Students are expected to verify the support they have received which is paid for through DSAs. Currently there are 3 verification methods agreed by SLC:

- A 'wet' (ink) signature of the student on a timesheet to confirm the hours have taken place
- Student confirms their support by logging into the support provider's system which has been built in prior agreement with SLC and meets criteria set out by SLC.
- An email from the registered email address of the student confirming when they have received supported

It should be noted that email verification should not be a primary verification method and should only be used where other verification methods have failed. This is because email is the least secure option.
Due to the growth in remote support services there has been an increasing need to look at alternative verification methods. This framework sets out the process for submitting a request to use electronically verified timesheets (or supporting documentation), the minimum information and data security requirements and expectations in the event of no verification.

Digital Signatures

A digital signature is the equivalent of a written signature. These come in many forms, including:

- Typewritten
- Scanned
- An digital representation of a handwritten signature
- A unique representation of characters
- A digital representation of characteristics, for example, fingerprints, retina scans
- A signature created by cryptographic means

Digital signatures are divided into three groups:

Simple Digital Signatures

- A simple digital signature may include (but not limited to):
- 'One time' password
- Scanned image of a signature
- Signature capture device*
- Tick box and declaration

These signatures are not necessarily unique nor are they under the sole control of the user; it may be possible that some contents could be altered without the document becoming invalid (such as the tick box example in the list above).

*Some software used in conjunction with such a device may change these signatures to Advanced or Qualified

Advanced Digital Signatures

- An advanced digital signature may include (but not limited to):
- Signature capture device in conjunction with software that meets advanced signature requirements
- E-Sign applications (Co-sign, DocuSign, Adobe Echo-Sign)

These signatures can identify the user, is unique to them, is under the sole control of the user and are attached to a document in such a way that it becomes invalidated if the contents are changed.

Qualified Digital Signatures

- A qualified digital signature may include (but not limited to):

- Cryptographic ‘keys’ such as Open PGP, PGP, GnuPG
- Smart Cards

- Biometric verification (Iris or retina pattern, finger prints)
- Mobile Phone dedicated software with highest level security certificate/encryption

These signatures meet all the requirements of an advanced signature with a digital certificate encrypted by a secure signature creation device.

Path to Live

SLC will consider proposals for digital verification if the digital signature is regarded as advanced or qualified. SLC are looking for verification methods that offer:

- **Authentication** - link the signatory to the information stated

- **Integrity** - allows changes to information provided to be detected easily

- **Non-repudiation** - ensures satisfaction (in a legal sense) about where the digital signature has come from

1. Any supplier interested in electronic verification should contact dsa_electronic_queries@slc.co.uk
2. This supplier pack is issued which outlines:
    - Standard Information Requirements
    - Security Specification
    - Authorising Signatures on behalf of students
3. You should then put together a proposal that outlines how students will electronically verify their timesheet/supporting documentation and how this will comply with all of the requirements set out in this supplier pack.
4. The proposal can be sent via email to dsa_electronic_queries@slc.co.uk. The email subject should include the name of the supplier and “Electronic Verification Proposal”.
5. The proposal will be reviewed by a management panel using the framework
6. We will share our thoughts and feedback on the proposal.
7. You must address any concerns raised by providing further documentation or clarification
8. Once we are satisfied the verification methods and submission documents are suitable, a ‘Go Live’ date will be agreed.
9. Upon the ‘Go Live’ date, you have permission to start submitting electronically verified timesheets with your invoices

Confirmation of the ‘Go Live’ date, an outline of the verification method and an example of the document agreed will be sent to our invoice team managers to cascade to our invoice teams ready for the first submission.

Any post ‘Go Live’ queries relating to the invoice and/or submission documents will fall into our business as usual processes.

Specifications

Detail	Requirements for Supporting Documentation	Comments/Actions
1	Supporting documents must have the following information; otherwise they may be rejected by SLC. ☐ Name of the company ☐ Support worker's full name ☐ Student's full name ☐ Student's CRN * ☐ Student's date of birth * ☐ Support type being claimed i.e. Note taker ☐ Date of when support was provided ☐ Start and finish times of each session ☐ Total number of hours being claimed per support type ☐ Must be identifiable who (ie student or authorised authority) has verified the support invoiced/evidenced on the supporting document ☐ Comments Box (eg - give detail of cancelled session or reason for 3rd party authorisation) ☐ Disclaimer detailing how information provided will be used (DPA) There are some additional pieces of information which are useful to have on the supporting document in the event of the document becoming separated from the invoice: ☐ Company's address ☐ Company's contact details ☐ Invoice number ☐ Invoice date	Supplier to adhere to all elements required. Any deviance from the requirements could result in additional work for both the Supplier and SLC. Where additional work is required to process, due to a deviance from these requirements, SLC may request that the Supplier returns to obtaining and providing written signatures as evidence. Data Protection caveat provided under point 9. *Require either/or both to ensure allocated to correct account/matching with invoice

Detail	Requirements for Supporting Email Verification	Comments/Actions

2	In order to submit an email as verification of support delivered, the email to the student must show: ☐ Sender's full name ☐ Sender's job title ☐ Sender's email address ☐ The date the email was sent ☐ The time the email was sent	Supplier to adhere to all elements required. Any deviance from the requirements could result in additional work for both the Supplier and SLC. Where additional work is required to process, due to a deviance from these requirements, SLC may request that the Supplier returns to obtaining and
	☐ The reason for the email/verification request ☐ Student's full name ☐ Student's CRN ***** ☐ Student's date of birth ***** ☐ Name of the company responsible for conducting the support (this could be the HEI) ☐ Support worker's full name ☐ Support type being claimed i.e. Note taker ☐ Date of when support was provided ☐ Start and finish times of each session ☐ Total number of hours being claimed per support type ☐ Comments Box (eg - give detail of cancelled session) ☐ Disclaimer detailing how information provided will be used (DPA) The student response must be included in the email submitted as verification of support. The student response must show: ☐ Student's full name ☐ The student's email address. This should be either the address they have registered with SLC or their HEI/course provider email address ☐ The date the email was sent ☐ The time the email was sent ☐ Must be identifiable that the student has clearly confirmed the support evidenced (in the detail provided in the email) requesting the verification.	providing written signatures as evidence. In the event of a dispute, we may request evidence that the support worker signed off their personal timesheets prior to verification being requested from the student. Data Protection caveat provided under point 9. ***** Require either/or both to ensure allocated to correct account/matching with invoice
Detail	**Submission Requirements**	**Comments/Actions**

3	☐ The supplier is responsible for ensuring only verified supporting documents are submitted to SLC ☐ A separate supporting document or verification email must be submitted per student ☐ The supplier is responsible for ensuring the correct supporting document is attached to the correct invoice ☐ For email verification, the subject line of the email (when submitting to SLC) must include: ○ Student full name ○ Student CRN ○ Description of contents (eg Student confirmation of support) ○ Corresponding invoice number	Multiple students showing on one supporting document or verification email will be rejected. Any system based solution employed must generate only single documents. Emails verifying support conducted should be submitted with the invoice – ie via post or e-invoices. They should not be submitted via dsa_electronic_queries@slc.co.uk or invoice_team@slc.co.uk unless specifically requested.
Detail	**Requirements for Systems requiring student log-in**	**Comments/Actions**
4	Students must have secure usernames and passwords/codes to access the system. Students must have access to technical support facilities including guidance on logging into the system, password resets, and navigational assistance as required.	Evidence that Students receive their unique log-in information securely should be demonstrated. Evidence that students can log in securely should be demonstrated. Evidence that the Supplier can provide technical support to Students, to assist them in logging into and using the system, should be demonstrated. Evidence that there is the ability to securely reset passwords and other secure information should be demonstrated.
Detail	**Requirements for Administrator Verification**	**Comments/Actions**

5	‘Administrator’ should be a named person from the company responsible for delivering the support to the student. ☐ Verification by an administrator should only be conducted with the express prior permission of SLC ☐ A request for administrator verification should be submitted to SLC in writing (email is acceptable) ☐ The administrator should be named to SLC in the permission request (this will be used for reference in the processing of the documents) ☐ The request should detail the reason why administrator verification is required ☐ The request should detail the prior steps taken to obtain student verification ☐ Any document submitted with administrator verification should include, as a separate supporting document, the written permission from SLC ☐ Any document submitted with administrator verification which does not include this written permission will be rejected ☐ In all cases, consent to authorise should be obtained from the student or evidence supplied to show the occasions this was attempted ☐ The student must be made aware that their support was verified by the	A HEP should provide a named administrator only if they are delivering support to the student. If the support has been contracted to a third party then it is the 3rd party that is responsible for obtaining the support verification. Administrators should therefore have the ability to verify support conducted. Administrator verification is to be an exception rather than the rule. SLC will review any agreements to electronic verification should the number of administrator verification requests be deemed too high. We may request that the supplier reverts to ink signatures. The Supplier should be able to demonstrate the workings of any above point should SLC request this. If ‘ink’ signed timesheets or supporting documents are available, then SLC expect that these will be submitted with the invoice. No administrator verification requests will be accepted if these documents are available.
	administrator. ☐ Should an Administrator verify the support conducted it must be made evident, on the resulting supporting document, that this has taken place ☐ SLC require details to be stated, on the timesheet, as to why the administrator signed on behalf of the student.	
Detail	**Requirements for Amendments**	**Comments/Actions**

6	☐ The student may dispute the information contained within the supporting document. ☐ Therefore any changes to the document should be recorded and sent back to the support worker. A new supporting document should be submitted to the student for their verification ☐ A non-editable copy of the verified document should be saved by the Supplier. This includes email verification.	There must be a clear process in place, and evidenced, that allows students to decline the details captured within the supporting document. Consideration should be given as to whether the supporting documents should be numbered if they are disputed. The revised document should be saved to comply with audit requirements.
Detail	**Requirements for Contingency**	**Comments/Actions**
7	☐ Contingency plans need to be in place should the on-line system fail. ☐ Contingency plans should prevent duplicate invoices and supporting documents from being generated and sent to SLC. ☐ Contingency plans should ensure that records are backed-up. ☐ SLC should be contacted in the advent of a systems failure.	The Supplier should be able to demonstrate the workings of any contingency should SLC request this.
Detail	**Requirements for Accessibility**	**Comments/Actions**
8	☐ Any method by which a student is required to verify support must comply with the Web Accessible Standards	It is important that students find the system, application or process straightforward.

Detail	Requirements for Data Protection	Comments/Actions
9	☐ Data protection regulations must be adhered to with regular audits conducted to ensure compliance. ☐ Suppliers shall be responsible for processing Personal Data and Sensitive Personal Data as Data Controllers to the Information Security Management standard (ISO 27001). ☐ Every supporting document must contain an appropriately worded data protection declaration. ☐ This declaration must be read and accepted by the support worker and student (both being Data Subjects). ☐ Suppliers must be registered with the Information Commissioner's Office. ☐ Suppliers must immediately notify SLC of any breach or potential breach of data.	For the purposes of compiling the information comprised within the timesheets, Suppliers shall be responsible for processing Personal Data and Sensitive Personal Data as Data Controllers (terms defined in UK GDPR) For the avoidance of doubt, Suppliers must be registered with the Information Commissioner's Office. Every timesheet must contain an appropriately worded data protection declaration, detailing how the Supplier will process the Personal Data and Sensitive Personal Data, including the sharing of the data with SLC. This declaration must be read and accepted by the support worker and student (both being Data Subjects), which acceptance should be unequivocal, whether as an integrated feature of the timesheet authorisation mechanism, or not. Suppliers must immediately notify SLC of any breach or potential breach of data giving full details to allow proper investigation and reporting within the 72 hour allowed time as per UK GDPR regulations.
Detail	**Requirements for Security**	**Comments/Actions**

10	☐ Standard security specifications must be in place as agreed by SLC Security Manager. ☐ We would expect all web based access to be HTTPS using at least 128 bit encryption. ☐ All users should have unique user ID and password. ☐ User maintenance should be a regular undertaking, archiving redundant users and enforcing password changes at regular intervals. ☐ Passwords should not be available to any other user (inc. privileged users) ☐ The system architecture should follow an 'n' tiered model for web based services (web/app/database), with appropriate separation of zones. ☐ The service should be fully auditable with interactions being written to log files, appropriate analysis of these logs in reasonable time and then offline storage and future interrogation.	The principles of Information Security Management standard ISO 27001 should be applied. Suppliers must take appropriate security measures to protect the service from either being accidentally or deliberately compromised; as a basic based on ISO 27002. The supplier must have an appropriate security policy and information assurance risk management regime in place to manage the service an assure customer and the SLC.
	☐ The service must be protected from vulnerabilities and exploits from the web or internal users through appropriate access controls (privileged users, network access controls etc), system configuration standards to minimise excessive services (hardened servers) and a maintenance routine to ensure future issues are addressed (patching etc). ☐ We assume the service and supporting infrastructure will be housed in an appropriate computing facility/data centre. ☐ Data integrity issues should be prevented as much as possible by appropriate controls at the time of collection (field types, formats and lengths etc). ☐ The service should be fully security tested (infrastructure, web application etc) prior to launch and after every major revision or at least annually	
Detail	**Requirements for Audit**	**Comments/Actions**

11	☐ Regular audits should be conducted by the Supplier. ☐ SLC reserve the right to conduct ad-hoc audits. ☐ If SLC asks it to do so, the Supplier will immediately make available to SLC any file, correspondence, document or information relating to the performance of the Supplier's obligations under this Agreement. ☐ Supplier is required to enable SLC to monitor or appraise the Services or the Supplier's ongoing ability to perform its obligations. ☐ In addition, the Supplier will make available any other information which is needed to enable SLC to comply fully and effectively with the requirements of any Regulatory Body. ☐ SLC or any representative of a Crown body or Regulatory Body may enter, and the Supplier will procure such entry to, the Supplier's premises or those of its agents, suppliers and subcontractors at all reasonable times to review all files, correspondence, documents or information and other things relating to the performance of the Services and to audit and inspect the Supplier's security arrangements and its compliance with the terms of this Agreement. ☐ SLC will give the Supplier a minimum of 48 hours notice where possible and except where access is required sooner as a result of the requirement of any Regulatory Body. ☐ Additionally the Supplier will give SLC and any representative of a	

	Regulatory Body reasonable help to understand the information provided by the Supplier, and SLC and any representative of a Regulatory Body will be allowed to have access to the Personnel. ☐ Following any audit or inspection carried out in accordance with Schedule, the Supplier will implement, as soon as reasonably practicable, any additional measures requested in writing by SLC. ☐ Where the additional measures affect the Supplier's subcontractors, suppliers and agents, the Supplier shall procure that those measures are implemented by the relevant subcontractors, suppliers and agents. ☐ Any file, correspondence, document or information provided by the Supplier pursuant to this Schedule will be treated as Confidential Information except to the extent it relates to the business or affairs of SLC. ☐ In addition to using its own employees, SLC may exercise its rights under this Schedule using external auditors or other agents.	

Administrator Verification Request

Administrator verification requests should be sent to dsa_electronic_queries@slc.co.uk.
These will be submitted to the invoice team managers for consideration. A response will be sent to the supplier confirming receipt and that the request has been submitted for consideration. The supplier will be notified of the outcome within 5 working days of the confirmation of receipt.

Below is a template which can be used to make such requests. This should help ensure we have the information required to consider the request.

Student Full Name	
Student CRN	
Student Date of Birth	
Type of support conducted **Date, times and number of hours conducted per support type – Plus a total number of hours** Eg. Specialist Study Skills 1st June, 9:00 – 10:30 (1.5 hrs) 4th July, 10:00 – 11:00 (1 hrs) TOTAL = 2.5 hrs Note-taking 2nd June 10:00 – 13:00 (3 hrs) 3rd June 13:00 – 16:00 (3 hrs) TOTAL = 6 hrs	
Are signed (in ink) paper timesheets available?	
Background or circumstance leading to no verification	
Details of actions taken If supplying copy emails please detail here the sender, date, time and subject line of each email as well as stating the outcome. Eg. *j.smith@uni.ac.uk* *10/07/2014 9:44* *"Please confirm timesheet for study skills support"* *No Response*	
Supporting Information/Additional File Notes	

Requested SLC Action	