Data Protection Policy

Business Area: Data Protection Office

Version: 8.0

Document Reference: POL-18-060

Document Control

Status: *Live*

Document Version History

Date	Version	Author	Comments
30/03/2004	0.1		Comments received.
	0.1		Comments received.
14/06/2004	0.1		Comments received.
16/01/2008	0.2		Comments received
15/02/2011	0.5		
21/07/2011	0.6		Amendment to SLC logo
14/09/2012	0.7		Change cross references and document titles
28/11/2012	2.4		Annual review and amendments made to policy, including revision of version control numbering.
11/12/2012	3.0		Published version
30/07/2014	3.1		Amendment to Data Protection Officer and policy owner details
03/10/2014	4.0		Published version
30/06/2015	4.1		Amendment to details of Data Protection Officer
30/06/2015	5.0		Published version
May 2018	5.1		Updates to reflect changes in data protection legislation
18/05/2018	6.0		Published version
30/01/2019	6.1		Update to new template. No content change
18/04/2019	6.2		Interim version - Annual review and amendments made to policy, including revision of version control numbering and RACI. Reviewed by DDPO & DPO.
03/07/2019	7.0		Published version
19/06/2020	8.0		Annual Review

Review and Approval Register

Note: RACI = R- Responsible, A- Accountable, C-Consulted, I-Informed

Name	Position	RACI Role
Gary Womersley	Data Protection Officer ("DP Officer") / Senior Information Risk Officer ("SIRO")	**A**
	Information Governance & Assurance Manager and Deputy DP Officer	**R**
	Information Governance & Compliance Manager/ Deputy SIRO	**I**
	Information Governance Officer (GDPR)	**C**
	Senior Manager – Legal & Compliance	**C**
	Senior Legal Executive	**C**

***NB: names of staff other than DPO have been removed under section 40(2) of the Freedom of Information Act 2000**

Update Schedule

The Data Protection Policy (the "Policy") is reviewed on an as needs basis but no less than once in any rolling 12-month period and may be amended at any time. The Data Protection Office ("DP Office") will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives. Recommendations for any amendments should be reported to the DP Office.

Applicability

The requirements in this document apply to all permanent, temporary and contract workers employed or engaged by SLC or any 3rd party organisations while at work or engaged on SLC business.

Compliance

- Any employee found to have violated this policy could be subject to disciplinary action, up to and including termination of employment.
- At its sole discretion, SLC may require the removal from the service provision account of any employee of a 3rd party organisation contractually engaged on SLC business who is found to have violated this Policy.

Contents

1 Overview

1.1 Introduction

Student Loans Company Limited ("SLC", "we", "us" and "our") is a non-profit making Government-owned organisation set up to provide loans and grants to students in universities and colleges in the United Kingdom ("UK").

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") and the UK Data Protection Act 2018 ("together referred to as Data Protection Legislation") regulates the processing of personal data and protects the rights of the data subject.

As SLC will collect, store and process personal data, we are registered as a data controller with the Information Commissioner's Office ("ICO") under registration number Z7261665, we are the data controller of any personal data that is provided to us. This means that we are responsible for deciding how we hold and use personal data. In certain circumstances, we may be a joint data controller. Please see the SLC Data Protection Statements/Privacy Notices for more detail.

Data Protection Legislation imposes restrictions on how we may use personal data.

1.2 Scope

1.2.1 The Policy applies to all data subjects in relation to whom SLC hold or have received personal data about in order to carry out SLC functions.

1.3 Status of Policy

This Policy sets out SLC's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal data.

SLC's designated DP Officer is responsible for monitoring compliance with Data Protection Legislation and this Policy. Any questions or concerns about the operation of this Policy should be referred in the first instance to the DP Office. Please refer to section 9 below for contact details.

If you consider that this Policy has not been followed, you should raise the matter with your line manager (for SLC staff) or the DP Office.

2 Data Protection Legislation

2.1 Background

2.1.1 Data Protection Legislation recognises the need to regulate the obtaining, retaining and processing of personal data in order to protect the interests of the individuals who are the subject of such personal data. Data Protection Legislation covers many data protection issues in detail and therefore you may find that guidance covering some aspects of data protection are set out in more detail in separate SLC policies and guidelines referred to within this Policy.

2.2 Definitions

2.2.2 There are a number of key definitions used within Data Protection Legislation that are essential to understanding this Policy and SLC's obligations under Data Protection Legislation.

- **"data"** – means information held in an electronic form (e.g. computers, personal organisers, laptops) or information held manually or in paper form as part of a relevant filing system. A **"relevant filing system"** means a filing system where information within that system relating to an individual can be easily found and is readily accessible.
- **"personal data"** – means any data from which a living individual can be identified or data which when mixed with other data or information held about the same individual would make it obvious as to who the subject of the data is. Examples of personal data include name, telephone number, age, qualifications and employment history.
- **"data controller"** – means a legal entity that determines the purpose and means of the processing of personal data.
- **"data processor"** - means a legal entity that processes data on behalf of the data controller.
- **"data protection officer"** - the DP Officer's primary role is to ensure that their

- **"data subject"** - means those living individuals about whom SLC hold personal details. Data subjects may include: staff, contractors, customers, job applicants, candidates and suppliers; and the data processed may relate to present, past and prospective data subjects.
- **"processing"** – means almost any kind of handling of data including but not limited to obtaining, collecting, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, transmitting, disseminating, aligning, combining, blocking, erasing or destroying.
- **"special category data**" – means data about a data subject's racial or ethnic background, political opinions, religious or similar beliefs, trade union membership, physical or mental health/condition or sexual life, criminal record or genetic or biometric data. Special category data can only be processed under strict conditions outlined in Data Protection Legislation.

2.3 Data Protection Principles

2.3.1 SLC has a duty to ensure that all personal data however collected is processed in accordance with the data protection principles detailed in the Data Protection Legislation.

2.3.2 Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, be kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay ('accuracy');

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

- and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.4 Special Category Data

2.4.1 SLC staff may become privy to special category data. Data Protection Legislation states that special category data should only be collected, processed, or disclosed in very specific circumstances as it is recognised that the processing of it may cause particular concern or distress to the data subjects.

2.5 Purposes of Processing

2.5.1 Please see the applicable Privacy Notice for information in relation to the purpose for which personal data is processed.

2.6 Data Retention

2.6.1 Please see the Records Management Policy for more detail in relation to the period for which personal data is retained.

2.7 Rights of the Data Subject

2.7.1 Data Protection Legislation establishes rights for data subjects with regard to the processing of their personal data including the right to:

- be informed about the collection and use of their personal data;
- obtain access to personal data (further details below at section 5);
- request to have certain personal data deleted or corrected;
- request certain personal data is restricted from processing. This enables the data subject to ask us to suspend the processing of personal data about the data subject, where for example the data subject wants us to establish its accuracy or the reason for processing;
- withdraw consent to the personal data being processed (where consent is relied upon by SLC);
- object to the processing of personal data;
- request the transfer of personal data to a third party; and
- complain to the appropriate supervisory body e.g. the ICO (further details below at section 10).

2.7.2 Further information on these rights, including how to exercise these rights, is available on the SLC Internet web pages.

3 Changes to Personal Data

3.1 Accuracy of Personal Data

3.1.1 SLC is required to maintain accurate records of the personal data it processes. Accuracy of personal data will be checked at regular intervals. It is also in your interest to keep your personal data up to date.

3.2 Changes to Personal Data

3.2.1 To assist SLC with its obligation to maintain accurate records, if any data subject's personal data changes this can be updated through one of the following channels:

- a customer, you can confirm/update your personal data using the self-serve online portal. If you are unable to access the portal, contact the appropriate support team. Contact information for customers is available at https://www.gov.uk/government/organisations/student-loans-company;
- an employee, contractor or other member of staff, and you cannot update your details through the employee self-serve function you should contact People@slc.co.uk or your agency;
- a supplier, please contact your relevant business contact within SLC;
- data subjects that do not fall within one of the aforementioned categories, should visit the SLC Internet web pages and choose the most appropriate contact channel.

4 Data Sharing

4.1 Sharing and Transferring of Personal Data

4..1 We may have to share personal data with third parties, including third party service providers. We require third parties to respect the security of that data and to treat it in accordance with Data Protection Legislation.

4.2 SLC will only transfer personal data outside of the European Economic Area ("EEA") in limited circumstances. SLC will, at all times, ensure that adequate technical and organisational safeguards are in place to ensure that any personal data transferred remains secure and is protected.

4.3 For Internal Use Only: If your role within SLC requires you to transfer data outside of the EEA, please discuss with the DP Office prior to initiating any such transfer.

5 Data Subject Access Requests ("DSARs")

5.1 Contact Points for DSARs

5.1.1 Individuals that SLC holds personal data about have the right to make a formal written request to access the data held. To submit a DSAR, follow the DSAR request channels outlined below:

5.1.2 For customers or individuals who are not staff:

Data Subject Access Requests
Verification Operations, 5 West
Student Loans Company Limited
100 Bothwell Street
Glasgow
G2 7JD

5.1.3 Staff/Former Staff – submit a request using via the Employee DSAR form available on the intranet or contact the People Department.

5.1.4 For Internal Use Only: All DSARs made to SLC should be notified promptly to the relevant department as a statutory time limit for responding applies.

6 Security Breaches

6.1 Notification of Security Breaches

6.1.1 A security breach (also referred to as a personal data breach) is considered to be a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If you become aware of a security breach or believe an event may constitute a security breach, you should raise this matter immediately with:

- for internal notifications: follow the internal SLC breach management procedure
- for external notifications: please follow the standard SLC complaints process

7 Enforcement by the ICO

7.1 ICO enforcement and Escalation

7.1.1 The ICO has certain enforcement powers provided under Data Protection Legislation, and may serve information, enforcement or monetary penalty notices on an organisation where it considers that Data Protection Legislation has been breached.

7.1.2 Data Subjects have the right to make a complaint to the ICO in relation to SLC's processing of personal data. The ICO's contact details are as follows:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

Email: casework@ico.org.uk Telephone: 0303 123 1113

7.1.3 For Internal Use Only: In the event that you receive a notice, or any other correspondence, from the ICO, you must refer this to the DP Office immediately.

8 For Internal Use Only: Offences

8.1 Failure to comply

8.1.1 While it is SLC's responsibility to comply with Data Protection Legislation, any failure by an employee, agent, contractor or other member of staff acting on behalf of SLC to comply with this policy or any other relevant SLC policies, procedures or guidelines may constitute a disciplinary offence.

8.1.2 Some activities may be considered gross misconduct; the following list gives some examples of such activities, but is not exhaustive:

- attempting to gain unauthorised access to restricted customer accounts as set out in the Accessing Restricted Customer Accounts Policy;
- unauthorised or unlawful obtaining, copying or disclosure of personal data under the control of SLC;
- unauthorised selling or offering to sell personal data under the control of SLC; and
- use of personal, or special category, data contrary to the purposes notified by SLC.

9 Contact Details

9.1 For further guidance on this Policy please contact SLC's DP Office:

Data Protection Office

Student Loans Company Limited

100 Bothwell Street

Glasgow

G2 7JD

Email: DPO@slc.co.uk

10 Related Documents

10.1 This document forms an essential part of SLC's overall policy framework and should be read in accordance with relevant related documents, including:

Document Description
Accessing Restricted Customer Accounts Policy
Records Management Policy
General Data Protection Regulation
Data Protection Act 2018

