Renate Gertz, Andrew Crossland

[Email address]

Protocol for Access to Data from the Corporate Student Record System

October 2017

**Protocol for Access to Data from the Corporate Student Record System**

## Purpose

The purpose of this protocol is to define the process and conditions for obtaining approval for access to student data, and the steps required before that data can be deployed.

## Introduction

This protocol relates to access to data from the corporate Student Record System (SRS), where that access is not provided via a front-end tool within the Student Systems supported portfolio.

Members of staff are provided with access to these services via individual UUN authentication, following appropriate authorisation and implementation of account access (see e.g. <http://www.euclid.ed.ac.uk/staff/NewsEvents/StaffAccounts.htm>) and/or the systems are managed directly by Student Systems.

It does include any access via a back-end process, whether directly or indirectly, to data owned by a corporate SRS system. Whilst this therefore covers traditional bespoke interfaces to a downstream system, or service providers wishing to access data via the generic interface, it also explicitly includes those who access the data from a downstream service (e.g. being supplied for another purpose). The main access will be via the EUCLID Interface database (hub).

## Background

On behalf of the University, the University Secretary is the senior owner of the corporate Student Record System (SRS). This responsibility is devolved to and is exercised operationally by the Director of Student Systems. Student Systems is the controller of EUCLID data, however delivered, and for as long as it exists.

The owner of the system has a duty to ensure that data are managed securely and appropriately, and that access is provided in keeping with the Data Protection Act and the University’s internal policies.

The owner also has a responsibility to ensure that only appropriate data are released, and that such data are delivered correctly according to agreed requirements.

## Request procedure

In the first instance, please contact:

Head of Student Systems
Lisa.Dawson@ed.ac.uk
(0131 6) 51 4593

Any requests for access must be approved by the Director of Student Systems. It is expected that Student Systems business and technical advice will be required when completing a request and as such support is available.

By requesting access you are agreeing to all points in section 5 about access to and use of data.

Any request must include a response to each item listed in sections 6, 7 and 8 which will be assessed for approval by Student Systems.

Once a request is approved the work will be will be assessed and prioritised against the existing programme of work within Student Systems.

After deployment Student Systems will write to the system owner annually to confirm that the position remains unaltered. Where an interface/access exists but the scope is to change, a further request is required.

## Access to and the use of data

By requesting access you are agreeing to the following:

* 1. The data must not be modified, amended or altered. Any data changes must be actioned within the Golden Copy.
	2. All users must agree to the terms and conditions for access to student data.
	3. Users must be strictly limited to those who have a legal basis for processing personal data. You can find the appropriate legal basis in the guidance document circulated along with this document.
	4. If the activity is statistical, data must be rounded or otherwise anonymised to prevent the identification of individuals.
	5. If the activity is not statistical but involves personal data and is for a different purpose from the purpose listed in the privacy notice, a new privacy notice must be provided to the data subjects.
	6. Staff using a receiving system must be trained in its use.
	7. The creation of a Security Code of Practice as per Information Security policy.
	<http://www.ed.ac.uk/information-services/about/policies-and-regulations/security-policies/security-policy>
	8. Any external disclosures of the data must be in accordance with <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/student-information>
	9. Any security or data breaches/losses must be reported to Student Systems and in accordance with the data protection breach management policy.
	<http://www.ed.ac.uk/records-management/data-protection/data-protection-policy>

## Data specification

List here exactly what data will be in the feed, both in terms of the data items and population. Please pay particular attention to any Special Categories of personal data about a subject’s health, race, ethnicity, religious beliefs, political opinions, trade union membership, genetic data, biometric data or sexual orientation.

## Data usage

* 1. Describe what the data will be used for, the legal basis for this use, and by whom it will be used. You can find the appropriate legal basis in the guidance document circulated along with this document.
	2. Define where the data will be obtained from. If not the EUCLID interface service, then either from EUCLID direct (so a bespoke interface) or from a system already fed from EUCLID.
	3. Detail the nature of the delivery of the data, including timings. E.g. If it will be instantaneous, via nightly/weekly download.
	4. Declare any intention of using the data for profiling, marketing or fundraising activities.
	5. For any special category data items such as data about a subject’s health, race, ethnicity, religious beliefs, political opinions, trade union membership, genetic data, biometric data or sexual orientation, provide particular justification and legal basis why access to these items is required.

## Data Governance Requirements

Please respond to each of the following points:

* 1. Nominate an individual responsible for the system and the data it contains.
	2. Declare whether a Data Protection Impact Assessment has been completed following the guidance available at [https://www.ed.ac.uk/records-management/guidance/checklist/data-protection-impact-assessment](%20https%3A//www.ed.ac.uk/records-management/guidance/checklist/data-protection-impact-assessment).
	3. Declare if the data will be supplied to any other system.
	4. Define a retention schedule for the data in this system as the data must be destroyed/permanently deleted when no longer needed and the manner in which the data will be destroyed
		+ - The receiving area must have written procedures for the use and deletion/destruction of the data.
	5. Define what testing steps (in terms of validity of the population and data items) will be undertaken and by whom.
		+ - In addition to other suitable testing steps, Student Systems staff must test the output against the specification, and sign it off before it can be deployed.
	6. Declare the use of third party service providers, which must be approved by student Systems.
		+ Any third party service involving the capability to view the data must be approved by Student Systems and must be governed by a contract containing the appropriate terms as specified at <http://www.ed.ac.uk/records-management/data-protection/guidance-policies/transferring-data>.
		+ If data is to go off site, Student Systems must quality assure and approve the population before development work commences. You must define each individual data item, and the purpose to which it will be used. Particularly sensitive data such as disability and ethnicity will require significant justification as to their essential need.
	7. Declare if the data will leave the European Economic Area.
		+ Transferring personal data to a data controller in a country outside the European Economic Area (EEA) must be authorised by Student Systems.

<https://www.ed.ac.uk/records-management/data-protection/guidance-policies/transferring-data/data-controller-non-eea>

* 1. Declare and describe any requirements for data transmission by email, fax or other method
		+ Any data transmission must be in accordance with the policy on taking sensitive information and personal data outside the secure computing environment.

<http://www.ed.ac.uk/records-management/data-protection/guidance-policies/encrypting-sensitive-data>

* 1. Declare the mechanism of system protection and access (e.g. Identity authentication via EASE authorisation).
		+ - Individual staff must have access approved by their line manager.
	2. Describe the procedure for dealing with subject access requests.
	3. Describe the procedure for dealing with rights of rectification, erasure and restriction.
	4. Describe the procedure for removing access from staff who leave or change job roles.

**Sarah Smith
University Secretary**

**October 2017**