Protocol for Authorisation for Access to Data, and deployment, where a Corporate Student Admissions and Curricula Systems is the Golden Copy

1. Purpose

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

2. Introduction

This protocol relates to access to data 'owned' by a corporate Student Record, Admissions and Curricula System (SACS), where that access is not provided via a front-end tool within the SACS supported portfolio.

It therefore excludes: access to EUCLID web, EUCLID client, PPMD, STUDMI, ADMISMI and associated reporting universes (delivered for example via BOXI). 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 SACS.

It does include any access via a back-end process, whether directly or indirectly, to data owned by a corporate SAC 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).

It should be noted that SACS is the owner of EUCLID data, however delivered, and for as long as it exists.

3. Background

On behalf of the University, the University Secretary is the senior owner of the corporate Student, Admissions and Curricula Systems (SACS). This responsibility is devolved to the Director of Academic Registry, and is exercised operationally by the Director of Student Admissions and Curricula Systems (SACS) within Academic Registry.

The owner of the systems has a duty to ensure that data is 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 is released, and that such data is delivered correctly according to agreed requirements.

Legal Framework

The Data Protection Act 1998 sets out how organisations can use personal data, that is, data about living, identifiable individuals. A SAC-managed system will contain personal data about students; this can include contact details, information relating to studies, funding information and data deemed 'sensitive', such as racial or ethnic origin. As such, the University must ensure that a corporate SAC system complies with the data protection principles.

The Act stipulates that the University tell students what information it holds about them, what it is used for and any other parties the information may be shared with. It includes requirements that students' information only be accessed and amended by authorised parties, that it be securely stored and protected, that the information collected is appropriate to the University's needs and not excessive, and that third parties do not have access to the information without

good reason and with appropriate security provisions in place. Students also have the right to access any personal data the University holds about them.

Failure to comply with the Data Protection Act can lead to the University being fined up to £500,000 or sued, and expose its students to risks including fraud, identity theft and distress. This could significantly damage the reputation of the University.

University's Policies

As part of initial matriculation with the University, students are notified that

"*The University of Edinburgh holds information about everyone who studies at the University. We use the information to administer your studies, maintain our IT systems, monitor your performance and attendance, provide you with support, monitor equal opportunities, make funding arrangements, to gather feedback (including via the National Student Survey), and for strategic planning. We disclose information about you to your funding body, the Student Loans Company, the Higher Education Statistics Agency and government bodies such as the Scottish Funding Council or the UK Borders Agency*."

The University must ensure that staff practices are in keeping with this statement

As part of access to a SAC-managed system, all staff must personally agree to:

(i) Comply with the Guidelines on the Disclosure of Information about Students: http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/guidance-policies/student-information

(ii) Comply with the Guidelines on the processing of mass emails and e-announcements: http://www.euclid.ed.ac.uk/staff/Policies/Mass_Email.htm

(iii) Comply with the policy on the Storage, Transmission and Use of Personal Data Outwith the University Computing Environment: http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/guidance-policies/encrypting-sensitive-data .

(iv) Comply with the University Computing Regulations:

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/computing-regulations

(v) Comply with the Information Security Policy:

http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/security-policies/security-policy

(vi) Comply with the Data Protection Policy:

http://www.ed.ac.uk/schools-departments/records-management-section/data-protection/data-protection-policy

Individual staff must also have access approved by their line manager.

4. Requirements

The following information is required in order for consideration of access:

a) Who is the receiving system owner? If different, who is the downstream system manager who will take responsibility for the data sourced from the SAC system?

b) Provide a summary of the purpose of the system(s) receiving the data

This should include the way in which the data will be used to administer students' studies (or otherwise meets the conditions under which the University has notified students that the data will be used).

c) Is the system supplied by a third party?

If a third party, what level of access will be available to staff of the third party? Will staff of the third party be able to take data off-site?

d) Will the data be held/hosted solely within the University and its infrastructure, and directly managed by the University?

If not and the data is hosted off site, then specific terms will require to be included within the University's contract with the third party.

Data Processed within the European Economic Area (EEA)

Records Management has developed "Contractual requirements for a transfer of personal data from the University to a data controller in the European Economic Area" (http://www.recordsmanagement.ed.ac.uk/InfoStaff/DPstaff/TransferringInformation/AnnexC.htm).

Model contract clauses are available at http://www.recordsmanagement.ed.ac.uk/InfoStaff/DPstaff/TransferringInformation/AnnexC.htm#ModelContract; model 2 is the normal approach.

Taking professional advice from Records Management, Academic Registry would require to approve the relevant clauses within each contract. An electronic copy of the contract must be lodged with Academic Registry.

The Director of SACS can provide examples of contract terms used previously with Third Parties receiving Personal Student Data within the EEA.

Data Processed outwith the European Economic Area (EEA)

http://www.recordsmanagement.ed.ac.uk/InfoStaff/DPstaff/TransferringInformation/EEACountries.htm#List notes:

"The eighth data protection principle set out in the Data Protection Act 1998 states that personal data must not be transferred to countries outside the European Economic Area (EEA) 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, or unless an exemption applies."

This scenario has not yet arisen within the University for Personal Student Data. Professional advice will be required from Records Management should a request be made.

e) Provision of a detailed outline of the population to be taken

e.g. which students are to be selected, the conditions for selection etc.

This would normally be prepared in consultation with Academic Registry SACS. Either way, Academic Registry SACS must quality assure and approve the population before development work commences.

f) Definition of each individual data item, and the purpose to which it will be used

Particularly sensitive data such as disability and address/telephone details will require significant justification as to their essential need.

This would normally be prepared in consultation with Academic Registry SACS. Either way, Academic Registry SACS must quality assure and approve the data items before development work commences.

g) 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, Academic Registry SACS staff must test the output against the specification, and to sign it off before it can be deployed.

h) Where will the data 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.

i) If appropriate (depending on the method of provision), what controls will be in place to ensure that only the authorised Student data items can be accessed?

j) What will be the nature of the delivery of the data?

   Will it be instantaneous, via nightly/weekly download etc?

k) Who will be accessing the data and for what purpose?

   Are those who will use the system aware that student data are confidential and cannot be released without the permission of the data subjects? How will it be ensured that those who access the data have been authorised to do so in terms of the processes for staff who apply for direct access to EUCLID?

l) What security arrangements will be in place to ensure that unauthorised individuals will not have access to student data?

m) Will the Data be secure in terms of the Data Protection Act?

n) Confirmation that the data will be used solely for the purposes described above, and will not be supplied to any other system without explicit authorisation from Academic Registry.

   SACS will write every year to the system owner to confirm that the position remains unaltered. Where an interface/access exists but the scope is to change, a further request is required.

o) Confirmation that the data delivered will not be modified, amended or altered

   Any data changes must be actioned within the Golden Copy.

p) Confirmation that processes are in place for data to be destroyed/permanently deleted when it is no longer required.

5. <u>How to Progress Approval</u>

   In the first instance, please contact:

   Barry Neilson
   Director of Student Admissions and Curricula Systems
   Academic Registry

   Barry.Neilson@ed.ac.uk
   (0131 6) 50 9160

Sarah Smith
University Secretary

June 2013