1. **Purpose**

The purpose of this protocol is to define the terms and conditions for individual access to student data.

1. **Introduction**

These terms and conditions relates to access to data from the corporate Student Record System (SRS) including all systems managed directly by Student Systems (EUCLID web, EUCLID client, STUDMI, ADMISMI and associated reporting universes delivered via BI Suite) and all downstream systems.

Members of staff are provided with access to Student Systems Supported 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).

It should be noted that Student Systems is the curator of EUCLID data, however delivered, and for as long as it exists and access to student data via any mechanism is subject to the following **Terms and Conditions:**

**Terms and conditions for individual access to student data regardless of data**

1. You must only access information about identifiable individuals when it is necessary for you to do your job.
2. You can only use the data for purposes associated with your job role.

(<http://www.ed.ac.uk/records-management/data-protection/data-protection-policy>)

1. You must follow the guidance on disclosing information about students when releasing student data to third parties. It may be a criminal offence to disclose this information in any circumstances.

(<http://www.ed.ac.uk/records-management/data-protection/guidance-policies/student-information>)

1. Do not access information about identifiable individuals on a screen that can be seen by other persons not covered by points 1-3.
2. Always lock your machine when leaving it unattended.
3. Only store data on University of Edinburgh systems and comply with university ‘Bring Your Own Device’ (BYOD) Policy: “*Use of Personally Owned Devices for University Work”*

(<http://www.ed.ac.uk/files/imports/fileManager/BYODPolicy.pdf>)

1. Printed documents containing student data must be securely destroyed to at least level 3 of the DIN 66399 destruction of data carriers standard

(<http://www.din-66399.com/index.php/en/securitylevels>).

1. Any download data should be stored on an access limited area of the University network, in Office 365 or on an encrypted device.

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

1. Follow local procedures for job role and handling personal data.
	1. When accessing data via a non-Student Systems delivered service, procedures described in *Protocol for Access to Data from the Corporate Student Record System* must be adhered to.
2. If using data from golden copy to populate another system, you must complete and adhere to the procurement document (<http://www.ed.ac.uk/student-systems/use-of-data/policies-and-regulations>)
3. You must adhere to the University of Edinburgh’s Confidentiality agreement.

(<http://www.ed.ac.uk/records-management/data-protection/guidance-policies/confidentiality>)

1. Comply with the Guidelines on the processing of mass emails and e-announcements:

(<http://www.studentsystems.is.ed.ac.uk/staff/Policies/Mass_Email.htm>)

1. Adhere to the University of Edinburgh’s Information Security Policy:

(<http://www.ed.ac.uk/information-services/about/policies-and-regulations/security-policies/security-policy>)

1. Adhere to the University of Edinburgh’s Computing Regulations:

(<http://www.ed.ac.uk/information-services/about/policies-and-regulations/computing-regulations>)

1. Adhere to the University of Edinburgh’s Data Protection Policy:

(<https://www.ed.ac.uk/records-management/data-protection/data-protection-policy>)