Student Information System (SITS) Client User Access Form

University of East Anglia

BLOCK CAPITALS PLEASE

Surname ……Forename……

School/Department ……..Job Title ……..

Telephone Number ……..Email …….....

UEA Username (eg ABC17DEF) …….....……..

Usernames and passwords are personal. You must not disclose your password to others or let anyone else access services using your password. Any attempt to gain unauthorised access to information or facilities, to try to disguise their identity or pretend to be someone else is prohibited and may be illegal under the Computer Misuse Act.

Please retain the second page of this document for your own records.

I agree to abide by the conditions of use described in this access form and confirm I have completed the Data Protection training (https://infregs-training.uea.ac.uk/dpa/)

Signed ……Date ……

Approved By (Name)…….. ……

Signature ……Date ……

Position ……

Temporary Staff only: Access from (date) ……...Access to (date)……..…..

Please indicate which Version of SITS the staff member will need access to:

SITS Version	LIVE ☐	DEV ☐	TEACH ☐	TEST ☐
If access to DEV, TEACH or TEST is required, enter additional information:				

Please indicate which parts of SITS the staff member will need access to. Please note that *Administrator* access is only given to staff who need high level access eg SIS Records team.

Admissions and Enquiries	Administrator *(high level access)*	☐	User *(standard write access)*	☐	Read-Only	☐	Enquiries Only	☐
Debtors	Administrator *(high level access)*	☐	User *(standard write access)*	☐	Read-Only	☐	Cashiers	☐
Student Records	Administrator *(high level access)*	☐	User *(standard write access)*	☐	Read-Only	☐		
Other (or if Administrator selected), enter additional information								

Would you like training to be arranged? Yes ☐ No ☐

Please log this completed form to the IT Service Desk: https://itsupport.uea.ac.uk/CherwellPortal/IT

For Internal Use

Received	SITS added	User Group	AD added
Version 3.1	SITS removed		BB

Student Information System (SITS)
Conditions of Use

As a user of the Student Information System (SITS) you have access to sensitive personal information as defined by the Data Protection Act. This information is confidential. You must adhere to the University regulations governing the use of computing facilities as described in the Conditions of Computer Use https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/usage-policies
Information used other than in the normal course of employment is an abuse of these policies and will be dealt with under the disciplinary procedures.

Disclosure of information must only be made on a need-to-know basis. Users must therefore not enquire, investigate or view the information contained within the SITS Student Record System unless directly required to do so for a specific task. Appropriate measures to keep information secure have been taken by the University. These measures provide an audit trail of use which will allow inappropriate use to be identified.

Measures must also be taken by users to ensure that information accessible from SITS is kept secure:

1. You must have completed the UEA Data Protection training (https://infregs-training.uea.ac.uk/dpa/) prior to requesting access to SITS.

2. The screen must be secured by a password screen lock when SITS is loaded and the user is not present in the room.

3. Offices which have access to SITS must be locked when SITS is loaded and when no one is present in the room. This can be via key, numbered key pad or swipe card.

4. Any spreadsheet or report downloaded on a PC containing confidential personal data must be encrypted with a password. The password must be in accordance with UEA password policies.

5. Encryption must be used when taking personal data off site by any means including use of mobile devices (including laptops), removable storage or emails to external email addresses to avoid the possibility of inadvertent and unintended disclosure to unauthorised third parties. Personal data must be transmitted or transported only in an encrypted form.

6. Should a laptop be required to access SITS then no data shall be stored permanently on the laptop. When the laptop is no longer required the laptop shall be wiped fully of all the confidential data before being passed to someone else to use.

Author	Corporate Information Systems Team
Creation Date	19/06/2017
Version No.	3.1