DATA MANAGEMENT PRINCIPLES FOR INFORMATION STRATEGY PROGRAMME V1.0

5/7/2016

Catherine McMillan

Data Management Principles for the ISC Programme

The systems and/or services that will be delivered by Projects within the ISC Programme should adhere to the following principles:

		Caveats
Avoid Duplication	No system should duplicate the functionality of an existing system	Unless a replacement project has been authorised
Cross University Approach	If a system is delivering functionality that is a "common need" then a cross University approach must be taken	Although a pilot can occur first so long as a deliverable will consider adoption for wider University approach
Ensure continuity	Any systems replacement must include migration and archiving of existing data.	Unless separate parallel projects are approved
Ensure continued interoperability	Any system replacement must include replacing existing outgoing interfaces to existing systems	Where those systems will be remaining after the implementation
Security	Meet the IT System/Services Cyber Security Compliance Policy	With documented and signed off Exceptions both for and by ISD and the data custodians.
Project Management	Align with University Project Management Principles	Unless an alternative approach is approved

Both projects within the ISC Programme and systems/services delivered by those projects must adhere to the following Data Management Principles.

		Caveats
Authentication	All production services must use the University's authentication services	
Common Identity	No system or service can duplicate identities for University staff, students or other stakeholders that already exist within the University's information architecture. Students will originate from	

	the Student Record System and staff from the HR System. This common identity being allocated from the University's Integration Hub.	
No duplication	No system should duplicate in isolation data that already exists within the University's Information architecture. Instead existing data should be securely utilised via an agreed and authorised API.	
Management Reporting	If deemed appropriate as part of an agreed and authorised delivery plan data must be provided to the University's Data Warehouse	Normally as a deliverable of the SuNBIRD Service
Legal Compliance	All data management must comply with legal requirements.	
Interface Management	All interfaces between systems should go via the University's Integration Hub.	Unless commercial or equivalent point to point interface is provided by a supplier and that they do not require an institutional identity.
Data Custodianship	Data custodians manage the access to data via APIs and Interfaces.	To be agreed by procedures throughout the process from the Business Case onward.
Data transfer on a 'Need to know' basis.	Data transfer must be minimised on a need to know basis. Data should only be transferred from a source system if required for business operations on the receiving system.	
Availability	All access should be role driven and must be appropriate for the current role. The correct access to do your job, your current job and no more.	