Imperial College
London

Imperial College

Data Protection Policy Code of Practice 6: Internal Data Sharing and Integration

Doc. Ref.	: Data Protection Policy Code of Practice 6: Internal Data Sharing and Integration
Version	: 0.4
Status	: Approved
Date	: 06/04/2022
Approved by	: Information Governance Steering Group
Review by	: 30/04/2024

1. Introduction

1.1 Purpose

1.1.1 This Code of Practice (CoP) provides the principles and process of how information in the College systems can be shared and/or integrated with other systems in line with College's Data Protection Policy. It describes how to raise a data sharing / integration request, and how this request should be reviewed, approved and processed.

1.2 Scope

All College information and data are in the scope of this CoP. The CoP is primarily aimed at information and data held in digital format, but the principles also apply to data held in other mediums, e.g. on paper.

The CoP applies to all College staff, students and authorised third parties.

1.3 Definitions and Principles

Source Information System: Information System **from** which information / data is requested to be shared and/or integrated into another system. A source information system can be an external system to the College.

Target (Destination) Information System: Information System **into** which information / data is requested to be shared / integrated. A target (destination) information system can be an external system to the College.

Principle 1: The source information system and target information system must be reviewed as part of a Data Protection Impact Assessment before a request can proceed.

Principle 2: The source information system must be the authoritative source for the data / information requested to be shared / integrated. That is, if a system is an existing target (destination) information system for the requested information / data, it cannot be used as a source information system for the same.

Principle 3: Data / information shared / integrated into the target information system must be designated as read-only. Any changes to information / data must be carried out on the authoritative system for that information / data, which should then be reflected on the target systems via sharing / integration methods. Similarly the data/information cannot be used to establish an alternative authoritative source.

2. Code of Practice

2.1 A request for data sharing / integration should be raised to ICT's Service Desk, and assigned to the Data Product Team. It should include the following information:

- The justification and business reason for the data sharing / integration request;
- Details of data/information requested to be shared/integrated and the source information system;
- Details of the target information system and how the data/information is intended to be used.

2.2 The Data Product Team will check and confirm that both the source information and the target information systems are known to the College. If not, they will arrange them to be reviewed. (See Principle 1 above). This may require a Data Protection Impact Assessment (DPIA) and/or ICT Architecture

Checklist to be carried out as required . They will also check that the request is consistent with the other principles contained in this CoP.

2.3 The Data Product Team will liaise with the Information Asset Owners of the relevant systems. If the Information Asset Owner(s) provide their approval of the use of data integration from/to their systems, the request will be passed to the relevant product line to be reviewed, prioritised and carried out according to the governance process.

2.4 When a data sharing / integration request has been completed, the sharing / integration interface will be recorded in the College IAR as an interface / data flow. This will ensure any dependencies can be discovered when changes are requested to source information systems.

2.5 It should be noted that responsibility for dealing with any future changes to the source information system, e.g. due to a system upgrade, lies with the information asset owner of the target(destination) information system. ICT will use reasonable endeavours to provide as much notice as possible of any changes to affected systems' information asset owners and information asset administrators. However, it may be necessary to make changes to source information systems due to urgent business reasons, even if the target information systems may not be ready for those changes.

Version History

Version/Status	Release Date	Comments
0.1/Approved	February 2019	Draft written by Mike Horner, Service Line Manager for Education as "ICT Data Integration Policy for Staff and Students". Reviewed by Service Line Managers (SLM) and Information Architects. Assigned to Mike Horner and Okan Kibaroglu, Head of Governance, to convert into a code of practice at the College Level with process clearly defined.
0.2/In Review	March 2019	Mike Horner and Okan Kibaroglu agreed that this should be included as a CoP under the College's Data Protection Policy. Robert Scott, Data Protection Officer, agreed that this could be introduced a CoP 6 under the policy. Updated by Okan Kibaroglu and Mike Horner as such for final review by the SLMs and Information Architects. Approved
0.3/In Review	August 2020	Name of the CoP changed to refer to "internal" data sharing. Following the reorganisation of ICT in July 2020, references to some of the ICT roles and responsibilities have been updated. Approved
0.4/In Review	March 2022	Reference to DART included Approved by IGSG