DPA CoP 06: Internal sharing and Integration

Introduction

1.1 Purpose

1.1.1 This Code of Practice (CoP) provides the principles and process of how information in university systems can be shared and/or integrated with other systems in line with 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

1.2.1 All university 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 like paper.

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

1.3 Definitions and Principles

1.3.1 **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 university.

1.3.2 **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 university.

1.3.3 **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.

1.3.4 **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.

1.3.5 **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.

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. If not, they will arrange them to be reviewed. (See Principle 1 above). This may require a Data Protection Impact Assessment (DPIA), completed via the university's Data Activity Risk-assessment Tool, and/or an ICT Architecture Checklist as required. They will also check that the request is consistent with the other principles contained in this CoP and associated policies.

2.3 The Data Product Team will liaise with the Information Asset Owner(s) 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 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.

Document Control

Document title:		DPA CoP 06: Internal Sharing and Integration	
Version:	2.1	**Date:**	November 2025
Initially approved by and date:		Information Governance Steering Group / March 2019	
Version approved by and date:		Data Protection Officer / November 2025	
Version effective from:		November 2025	
Originator:		Division of the University Secretary	
Contact for queries:		Data Protection Officer	
Cross References:		Data Protection Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx Information Security Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/Information-Security-Policy-v7.0.pdf Information Governance Policy Framework / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Information-Governance-Policy-Framework---to-be-reviewed.pdf	
Notes and latest changes:		February 2019 V0.1 - Draft written March 2019 V0.2 - Approved by IGSG August 2020 V0.3 - Amended title - Corrected team names March 2022 V0.4 - Reference to DART included - Approved by IGSG February 2025 - Updated to meet new brand standard November 2025 V2.1 - Removed hidden URLs to improve accessibility	