Oxford Policy Management

Data Ownership and Usage in Oxford Policy Management

Table of Contents

1 Introduction

The objective of this policy is to provide OPM employees and any externals working with OPM guidance on how to treat information they come into contact with that is, or can reasonably be regarded as, confidential to OPM or our clients, partners and any other external parties.

1.1 Scope of the Activity

These procedures apply to any information, data, diagrams, etc. which personnel (including OPM staff, subcontractors, other suppliers, partners etc.) become aware of, or come into their possession that is marked as “Confidential”, that they are told is confidential, or that they ought reasonably to know is confidential.

2 Procedures

2.1 Roles & Responsibilities

Chief Information Officer	This person is responsible for ensuring that this policy is, and remains fit for purpose.
Project Manager	This person is **responsible** for ensuring the adherence to this policy by all project personnel during the life of the project and upon its termination.
Project Personnel	Everyone working on a project has a responsibility to ensure that confidential information is treated in accordance with these guidelines.

2.2 Possession of Confidential Information

During the life of a project, project personnel must respect the confidential nature of OPM's information and that of their partners and clients.

If you come into the possession of confidential information:

1. You must store all data within your internal hard disk, this will ensure that the data is encrypted appropriately.
2. Ensure that it is kept secure (either in lockable storage if it is in hard copy, or on OPM platforms if it is electronic).
3. Do not view it in public locations or discuss it in public locations, such as on public transport or in public meeting places.
4. Do not remove any "Confidential" notices on the information

If you need to disclose any confidential information:

1. Ensure that you have the information owner's permission to disclose the confidential information
2. Only ever disclose the information to people who have an absolute necessity to know it in order to carry out their duties for a project
3. Ensure that they are aware of the confidential nature of the information, and that they are provided with, and comply with, this policy.

2.3 Unauthorised Disclosure

If at any time you become aware of an unauthorised disclosure of confidential information, you must follow these steps:

1. Immediately put into motion any actions you can to mitigate the damage of the disclosure and to retrieve the information, such as requesting the immediate deletion (and proof of deletion) or return of the confidential information and revoking access to a file if access has been granted to someone in error.
2. Immediately inform the information owner and comply with any instructions they give you
3. Inform the Project Manager, detailing exactly what has been disclosed, and the potential consequences of this. The Project Manager will escalate to the Risk and Compliance Manager if necessary.

2.4 At the end of the Project

You must seek advice from the information owner on the process to follow, this may include:

1. Returning to them all copies of the confidential information
2. Deleting all the confidential information
3. Providing certification that all copies of the information have been deleted.

Oxford Policy Management

Data Ownership & Usage

Document Purpose:

The objective of this policy is to provide OPM employees and any externals working with OPM guidance on how to treat information they come into contact with that is, or can reasonably be regarded as, confidential to OPM or our clients, partners and any other external parties.

Policy Overview			
Policy Owner	Chief Information Officer		
Applies to	All OPM Representatives		
Global or local scope	Global		
Version Number	1.0	**Effective from**	20.10.2017
Approvals (Dates)	**Board**		N/A
	Policy Authorisation Committee		N/A
	Other (please state)		N/A