|  |
| --- |
| Data Integration Platform  DIP Subsidiary Document  DIP Data Management  DSD006  Version 0.6  Date: DD Month YYYY |

DSD006 relating to data management in regards to the DIP.

1. Reference is made to the DIP Supplement of the Balancing and Settlement Code.

2. This is DIP Subsidiary Document DSD006, Version 0.6 relating to data management requirements for DIP Users wishing to use the DIP.

3. This DSD is effective from DD Month YYYY.

4. This DSD has been approved by the DIP Manager.

**Amendment Record**

| Version | Date | Description of Change | Approval Reference |
| --- | --- | --- | --- |
| 0.1 |  | Initial draft for Workgroup review | - |
| 0.2 |  | Second draft for Workgroup review | - |
| 0.3 |  | Issue 101 Consultation | - |
| 0.4 |  | Issue 101 Report | - |
| 0.5 |  | Shared with Ofgem | - |
| 0.6 |  | P474 | - |

**Contents**

[1 Introduction 5](#_Toc169521670)

[1.1 Scope and Purpose 5](#_Toc169521671)

[2 Data Management 6](#_Toc169521672)

[2.1 General requirements 6](#_Toc169521673)

[2.2 Data Protection Assurance 6](#_Toc169521674)

[2.3 Personal Data Breach 6](#_Toc169521675)

[3 Open Data Policy 8](#_Toc169521676)

[3.1 Application 8](#_Toc169521677)

[3.2 Data release principles 8](#_Toc169521678)

[3.3 Data release process 8](#_Toc169521679)

[3.4 Data Triage and Mitigation 9](#_Toc169521680)

# Introduction

## Scope and Purpose

The purpose of this DSD is to set out the rules and processes the DIP Participants are expected to adhere to in relation to the DIP.

Data Management ensures that the relevant legislation is adhered to with regards to the protection of data.

The rules, processes and procedures are the minimal level to be adhered to and can be exceeded should individual organisations wish to.

# Data Management

## General requirements

DIP Participants shall adhere to the Authority’s ‘Data Best Practice Guidance’.

## Data Protection Assurance

Without prejudice to DSD003 ‘Assurance and Reporting’ the DIP Manager may undertake audits of DIP Participant’s compliance with this DSD.

DIP Participants shall provide such information (including copies of data protection policies, privacy policies and data protection impact assessments), co-operation, and assistance in relation to any request made by the DIP Manager (or any third party appointed by it to undertake such assurance activities, or its or their representatives) as the DIP Manager may reasonably require to demonstrate adherence to the DIP Rules in respect of any system interacting with the DIP.

For the avoidance of doubt, the purpose of such audits shall be to provide assurance that DIP Users have relevant policies and procedures in place. The DIP Manager provides no warranty to any DIP User (or to DIP Users as a whole) that a DIP Users policies and procedures are appropriate or fit for purpose.

## Personal Data Breach

In the event of a Personal Data Breach, where such breach relates to use of the DIP, DIP Users should inform the DIP Manager as soon as practicable and keep the DIP Manager informed as each action is taken.

Where a Personal Data Breach **may** impact more than one DIP User, the DIP Manager shall take all reasonable endeavours to ensure relevant information is passed to the required organisations, and actions are aligned in respect of potentially impacted DIP Users. So far as practicable, the DIP Manager shall pass information as soon as it can so that other DIP users may report within the required time frames.

Where the DIP Manager (or DIP Service Provider) identifies a Personal Data Breach (whether their own breach or somebody else’s) they shall liaise with the relevant DIP Users to ensure requisite actions are taken (including compliance with any legal requirements).

Dependent on the nature of the Personal Data Breach the DIP Manager may:

1. notify some, or all, DIP Users of the situation. DIP Users should immediately follow any instructions issued by the DIP Manager to mitigate the risk of the security incident;
2. Suspend a DIP User’s access in accordance with DSD002 ‘DIP Connection and Operation’ with no prior notification;
3. notify the Information Commissioner’s Office of the data breach; and
4. notify the police or other appropriate agency or body of the data breach.

# Open Data Policy

## Application

The DIP Manager will not access data contained within Messages and Publications other than where specifically described in DSD003 ‘Assurance and Reporting’. However, they will hold data relating to DIP performance and DIP Users activity (e.g. number of each type of message sent). Any data held of this nature will be for the purposes described elsewhere in these DIP Rules and will only be shared with the organisations listed in DSD003 and this section.

The requirements in this section shall apply to the DIP Manager primarily, but should be used as guidance/advice for DIP Users when implementing their own open data policy.

## Data release principles

The default shall be that all open data requests shall be met subject to the further provisions of this section.

Data requests shall be subject to Data Triage and Data Mitigation to determine whether any actions need to be taken to make the data releasable i.e. so that there is no impact on the data subject or people connected to them.

In considering whether data can be released, consideration shall be given to, and advice/permission sought from, the owner of the data and the owner of the Meta Data (if different).

The DIP Manager shall consider whether the data requested is already available from other sources and, if applicable, shall direct the applicant to those sources.

The cost for releasing data may be recoverable from the person/organisation requesting that data. However, consideration shall be given to the wider industry benefit of making a data-set publicly available, and not just to the original requester, this shall include regular re-publishing/update of such data set.

## Data release process

Where the DIP Manager holds the data requested by virtue of being DIP Manager e.g. the number and type of DIP Users, they shall follow the requirements of this DSD.

Once the DIP Manager has completed classification, Data Triage and Data Mitigation (see below) they shall consider whether there is value to be gained from consulting industry prior to publishing the data set.

The DIP manager shall publish their decision to release the data set, and where applicable, publish it. They shall not release and/or publish the data set until at least 10 WD after publishing their decision in order to allow for appeals to be raised as per DSD001 ‘DIP Governance’.

## Data Triage and Mitigation

When reviewing an application to release data, the data set requested, the initial level of access shall be classified according to one of the following definitions:

1. Open – Data is made available for all to use, modify and distribute with no restrictions;
2. Public – Data is made publicly available but with some restrictions on usage;
3. Shared – Data is made available to a limited group of participants possibly with some restrictions on usage; and
4. Closed – Data is only available within a single organisation.

The definitions are based on the Open Data Institute’s data spectrum and shall be reviewed by the DIP Manager at least annually to ensure the DIP Rules align with industry best practice.

Once initial classification has occurred, triaging shall follow. This is the process by which actions to de-classify a data set can be identified. Consideration shall be given to without limitation:

1. Would the data set be less sensitive but retain its value after anonymisation / redaction?
2. Can risk be reduced by requiring licence restrictions?
3. Can risk be reduced if shared with a limited group or licence restrictions?
4. Can limiting audience or imposing licence restrictions reduce commercial risk?

Once the data has been triaged, mitigating actions shall be applied. Mitigation can include, but not be limited to:

1. Redaction – Removal of sensitive data;
2. Anonymisation – Removal of personal data;
3. Aggregation – Combine data sets so the collective sum is less sensitive;
4. Limitation – Only share with specific individuals or group(s);
5. Noise – Combine original data with meaningless data to confuse;
6. Delay – Wait until data is less sensitive before sharing;
7. Differential Privacy – Obscuring the data in such a way as to mask original identities;
8. Shift/rotate – Altering the position or orientation of spatial or time series data;
9. Randomisation – Making random changes to data; and
10. Normalisation – Modifying data to reduce the difference between individual subjects.

Following Mitigation, the requested data set shall be re-classified and, if deemed appropriate be subjected to further triage and mitigation until all stakeholders are in agreement that the correct classification has been achieved for the data set to meet the purpose for which it was requested.

The DIP Manager shall be obliged to produce open data guidance to complement the contents of this DSD which may be used by other DIP Participants in relation to their own open data policy.