Upper Medway Internal Drainage Board

Subject Access Request Policy

1. Scope

All personal data processed by the Upper IDB is within the scope of this procedure. This procedure excludes personal data that is asked for as a matter of routine by data subjects.

Data subjects are entitled to ask:

- Whether the Upper IDB is processing any personal data about that individual and, if so, to be given:
  - a description of the personal data;
  - the purposes for which it is being processed; and,
  - details of who will be allowed to see the personal data.
- To be given a copy of the information and to be told about the sources from which the Upper IDB derived the information; and
- Where appropriate, logic involved in any automated decisions relating to them.

2. Responsibilities

The Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting on Subject Access Requests (SARs).

The Data Protection Officer is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests can be made verbally, or in writing.

3.2 The data subject must provide evidence as to their identity.

3.3 The data subject must identify the data that is being requested and where it is being held and this information must be shown on the SAR application form. Note that the data subject is entitled to ask for all data that the Upper IDB holds, without specifying that data.

3.4 The date by which the identification checks, and the specification of the data sought must be recorded; the Upper IDB has one month (30 days) from this date to provide the requested information. There are some circumstances in which an extension to that one month will be provided, (excessive request) however failure to inform the data subject as to the extension would in itself be a breach of the GDPR.

3.5 The SAR application should be dealt with by the Data Protection Officer, who will ensure that the requested data is collected within the time frame.
Collection will entail either:

- Collecting the data specified by the data subject, or
- Searching all databases and all relevant filing systems (manual files) in the Upper IDB, including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives. The CEO maintains a data map that identifies where all data in the Upper IDB is stored.

3.6 The Data Protection Officer maintains a record of requests for data and of its receipt, including dates. Note that data may not be altered or destroyed in order to avoid disclosing it.

3.7 The Data Protection Officer is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

3.8 If the requested data falls under one of the following exemptions, it does not have to be provided:

- Crime prevention and detection.
- Negotiations with the requester.
- Management forecasts.
- Confidential references given by the Upper IDB (not ones given to the Upper IDB).
- Information used for research, historical or statistical purposes.
- Information covered by legal professional privilege.

3.9 The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

3.10 The electronic formats used for responses to SARs are:

- PDF file.

November 2022 Alterations

- Removed reference to LMIDB
- Minor formatting