Upper & Lower Medway Internal Drainage Board's
Breach Notification Policy

1. Scope

1.1 This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

1.2 The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and Councillors of Upper & Lower Medway IDB are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. Procedure – Breach Notification Data processor to Data Controller

3.1 Upper & Lower Medway IDB shall report any personal data breach to the data controller (CEO or designated Data Protection Lead) without undue delay.

3.2 Data Protection Lead, records breach in the Internal Breach Register.

3.3 Notification between parties is made by [email, phone call, etc.].

3.4 Confirmation of receipt of this information is made by email.

4. Procedure – Breach Notification Data Controller to Supervisory Authority

4.1 Data Protection Lead shall notify the supervisory authority [ICO] without undue delay, of a personal data breach.

4.2 Data Protection Lead assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

4.3 If a risk to the aforementioned is likely, Data Protection Lead shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

4.4 The data controller (CEO) shall provide the following information to the supervisory authority on a Breach Notification Form:

4.5 A description of the nature of the breach.

4.6 The categories of personal data affected.

4.7 Approximate number of data subjects affected.

4.8 Approximate number of personal data records affected.

4.9 Name and contact details of the Organisation.

4.10 Likely consequences of the breach.

4.11 Any measures that have been or will be taken to address the breach, including mitigation.

4.12 The information relating to the data breach, which may be provided in phases.

4.13 Data Protection Lead notifies their contact within the supervisory authority, which is recorded in the Internal Breach Register.

4.14 Notification is made by [email, phone call, etc.].

4.15 Confirmation of receipt of this information is made by email.

5. Procedure – Breach Notification Data Controller to Data Subject

5.1 Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject the Upper & Lower Medway IDB shall notify the affected data subjects without undue delay.

5.2 The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.5 above.

5.3 Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

5.4 The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

5.5 It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

5.6 The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.