

**Data Breach Procedure - rev 0**

**Data Breach/Suspected Data Breach**

It is important that any personal data breaches, or indeed suspected breaches, across the Tay Road Bridge Joint Board are reported as soon as possible to the Information Commissioner’s Office. Under the terms of the General Date Protection Regulation (GPDR), data controllers have no longer than 72 hours to report a breach to the Information Commissioner’s Office after having become aware of it.

If a breach (or suspected breach) has occurred then staff should follow the flow chart as detailed in Appendix 1. The table in Appendix 2 – Data Protection Breach Question/Answer Form should be completed as fully as possible by staff member(s) who are aware of the breach in order that all information can be gathered.

For more information refer to the latest ICO Breach Reporting Document found at https://ico.org.uk

**Notification of a Personal Data Breach to the Information Commissioner’s Office**

In the case of a personal data breach, the controller, Tay Road Bridge Joint Board shall, without undue delay and certainly no later than 72 hours after having become aware of it, notify the Information Commissioner’s Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In cases where a notification to the Information Commissioner’s Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification to the Information Commissioner’s Officer should document:

* description of the nature of the personal data breach including (where possible), the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
* the name and contact details of the Tay Road Bridge Joint Board’s Data Protection Officer or other contact point where more information can be obtained;
* the likely consequences of the personal data breach; description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The above information should be provided without undue delay. This documentation will enable the Information Commissioner’s Officer to verify compliance.#

## **Communication of a Personal Data Breach to the Data Subject**

If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Tay Road Bridge Joint Board will communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and any measures taken by Tay Road Bridge Joint Board to contain the breach.

Communication to the data subject(s) shall not be required if any of the following conditions are met:

* the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
* the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
* it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller, Tay Road Bridge Joint Board, has not already communicated the personal data breach to the data subject, the Information Commissioners Officer, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

**Data Breach Review**

The Tay Road Bridge Joint Board commit to undertaking a high level review of any data breaches in order to understand where weaknesses in procedure may be present and amend procedures as required to prevent reoccurrence. This will be carried out within one calendar week of the data breach.

**Appendix 1 – Data Breach Procedure – Flow Chart**

****

**Data Breach Reporting Flowchart**

**Breach / Suspected Data Breach**

Staff Member Aware

Advise Bridge Manager and DPO a.s.a.p.

Advise Individual(s) Affected Without Undue Delay

Bridge Manager

To:

Report to ICO in full

and

Advise DPO in full

The Bridge Manager logs this and details reasons for not reporting

The Bridge Manager logs this and details reasons for not reporting

No

No

Yes

Yes

Is the incident significant and likely to pose risk to an individual(s) or the TRBJB?

Is the incident very minor and unlikely to pose a risk?

i.e. Pseudonymised Data

Data Protection Breach Question/Answer Form to be sent to Bridge Manager and DPO

Data Protection Breach Question/Answer Form to be Completed by Reporting Staff Member and Line Manager

Report to Relevant Line Manager

**Appendix 2 – Data Protection Breach Question/Answer Form**

|  |
| --- |
| 1. When did the incident/data breach happen – date, time, location and item(s) involved?
 |
| 1. How many people are likely to be affected/at risk?
 |
| 1. What kind of data is at risk? How can it potentially affect the individuals in question?

(Consider various aspects including emotional, financial, personal loss, etc.) |
| 1. Describe the likely consequences of the personal data breach if at all possible.
 |
| 1. Please provide details of how the incident happened?
 |
| 1. Has a similar incident happened before? If yes, please provide dates and details.
 |
| 1. Are the individuals involved aware of what happened? If yes, how did they find out?
 |
| 1. What actions have you taken so far as a result of the data protection act?
 |
| 1. Has the data been recovered? If no, what is being done to recover the data?
 |
| 1. Who else knows about the breach in question?
 |
| 1. Details of the person reporting the incident (Name/Position/Department)
 |

Please send this completed form as soon as possible to: alan.hutchison@tayroadbridge.co.uk

The Data Protection Officer for the Tay Road Bridge Joint Board is:

Ian Smail, Dundee City Council

The Bridge Manager, Alan Hutchison, will liaise with the Data Protection Officer.