Tay Road Bridge

DATA PROTECTION POLICY

Prepared by:	A Hutchison
Reviewed by:	K McKaig

Document Reference:	**TRB 04 rev 0**
Approved for Issue:	**12 August 2015**
Date:	Bridge Manager

TAY ROAD BRIDGE JOINT BOARD

DATA PROTECTION POLICY

1. INTRODUCTION

In order to carry out is functions the Tay Road Bridge Joint Board needs to collect and use information about people, including members of the public, current, past and prospective employees and suppliers.

The Board is committed to protecting the privacy and rights of all people it holds information about. It regards the fair and lawful treatment of personal information as essential to its operations and to maintaining confidence and trust in the Board. The Board will encourage and promote a culture of awareness of the Data Protection Act 1998 and its guiding principles. It will ensure that it treats personal information lawfully and correctly however it is collected, recorded and used and whether the information is on paper, in computer records or recorded by any other means.

To this end the Board fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 (the Act).

The Data Protection Act 1998 regulates the processing of information relating to living persons in the UK. It requires that data controllers be registered with the UK Information Commissioner and comply with the **eight principles** which are legally enforceable. The Principles require personal data files to be up-to-date and accurate and that procedures are established which enable the Board to fully answer enquiries from persons about the data which the Board holds about them.

Terms of reference within this policy (e.g. 'personal information', 'subject access request') are used with the same intent as the definitions applied within the Data Protection Act 1998.

2. THE DATA PROTECTION PRINCIPLES

Personal information held on or produced by computer (for example, printed paper, digital files, CDs or CCTV), as well as information in paper files, is protected by the Data Protection Act 1998. Under that Act, the personal information held by the Board must be:

- processed fairly and lawfully;
- obtained and processed only for one or more specified lawful purposes;
- adequate, relevant and not excessive;
- accurate and kept up to date;
- not kept for longer than is necessary;
- processed in line with the rights of the person the information is about;
- processed with due regard to security; and
- will not be transferred to a country outside the European Economic Area unless special conditions are met.

3. SCOPE

The data protection policy ('the policy') will apply to all Board Members, Officers and employees.

The policy is applicable to all personal data/information processed by the Board.

It is the Board's policy to fully comply with the Data Protection Act 1998 and all other related statutory, criminal and civil obligations to which the Board is required to adhere. This applies to the retrieval, storage, processing, retention, destruction and disposal of 'personal information'.

The policy will be reviewed every three years and, if appropriate, amended to retain its relevance.

4. ROLES AND RESPONSIBILITIES

The Bridge Manager is responsible for developing, maintaining and administering the data protection policy. He is also responsible for all aspects of compliance with the Act, and associated legislation, and will develop appropriate procedure for the purpose of controlling adherence to the Data Protection Act 1998.

5. ROLE OF BOARD MEMBERS, OFFICERS AND EMPLOYEES

Board Members, Officers and employees will only have access to personal information where that access is essential to their duties.

Employees should discuss with the Bridge Manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by an employee.

Employees with access to personal information must be familiar with the requirements of the Data Protection Act 1998. Employees should only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

Board Members, Officers and employees must all follow good practice as indicated by the Data Protection Act when processing personal data.

6. ADVICE AND TRAINING

The Board will provide advice and training for employees to comply with this policy.

7. NOTIFICATION

The Board will ensure that it maintains its Notification entry with the Information Commissioner on an annual basis. A mechanism will be put in place to ensure the notification entry is reviewed regularly and kept up to date.

8. SUBJECT ACCESS

The Bridge Manager is responsible for processing subject access requests on behalf of the Board. Each individual employee is responsible for passing any subject access requests received to the Bridge Manager as soon as possible.

The Board will endeavour to process all subject access requests within the statutory forty day deadline. Where the Board is unable to process the request within the timeframe, the data subject should be notified as soon as possible of any potential delay, the reasons for such a delay, and the date when their information will be made available.

A fee of £10 will be applicable for subject access requests made by members of the public. The Board will not charge a fee for employees wishing access to information relating to them in the course of their employment.

9. PROCESSING OF PERSONAL INFORMATION

The Data Protection Act applies to personal information processed by any forms of medium, including CCTV images, photographs, and digital images. Any processing of such data must be in accordance with the principles of the Data Protection Act and this policy.

10. COMPLIANCE

The Bridge Manager will be responsible for carrying out a regular review of all areas of the Board to ensure compliance with the policy.

All employees have a responsibility to report suspected breaches of the data protection policy to the Bridge Manager, who will liaise with the Clerk to the Board as to the handling of the breach or potential breach. All breaches or potential breaches ae to be recorded, risk assessed and corrective measures put in place to ensure continued protection of personal data.

Any employee who is found to have inappropriately divulged personal information will be subject to investigation under the Board's disciplinary procedure, which may result in dismissal and possible legal action.

11. DISCLOSURE OF DATA

The Board must ensure that personal information is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal information held on another individual to a third party.

The Guidance attached to this policy contains advice on sharing of personal information and Board Members, Officers and employees must all follow it when considering whether or not to share.

If a request is received from Police Scotland for the disclosure of personal information, for the purposes of prevention and detection of crime, then the information should only be disclosed where a Police Scotland Request for Disclosure of Personal Data form has been completed and submitted to the Board.

12. INFORMATION SECURITY

All staff are responsible for maintaining appropriate security for the personal data to which they have access to.

13. RETENTION AND DISPOSAL OF DATA

The Board aims to ensure that personal information is not retained for longer than necessary. Personal data must be disposed of in a way that protects the rights and privacy of data subjects such as shredding, disposal as confidential waste, and secure electronic deletion. All systems should be reviewed on a regular basis to identify records which are no longer required and these will be destroyed securely.

Guidance for Staff on Sharing Personal Information

We all have a duty to protect information the Board holds about individuals. This information can include names and addresses for customers or information about members of staff.

The following principles will help staff when making decisions about sharing or using information.

1. **Is the sharing justified?**

   You have to have a good reason for sharing personal information and this must be a reason you can explain.

   Do not share information just because you think others have the right to know that information or you like to tell people about what has happened at work. Only share the information where it is necessary and reasonable to do so.

2. **Do you have the power to share?**

   Consider the following:-
   - The type of organisation you work for
   - Any relevant functions or powers of the Board
   - The nature of the information you have been asked to share (for example was it given in confidence?)
   - Any legal obligation to share information(for example a statutory requirement or a court order)

3. **If you decide to share**

   Key points to consider:-

   - Only share what is necessary
   - Share information securely
   - Consider if you have to tell the individual that you have shared their information

   When it is essential or in the best interest of the person to share, then only the particular facts around the cause for sharing should be given.

4. **Record your decision**

   If you share information you should record:-

   - What was shared and for what purpose
   - Who it was shared with and when
   - Your justification for sharing
   - Whether it was shred with or without consent

5. **Access to personal information should be on a strict need to know basis.**

   Only those staff members who need access to personal information should have access to it. This could be in order to undertake tasks within their job role, or tasks which they have expressly been given responsibility for.

   This applies when sharing information also. You should only share the concerns or information you have with those you consider need to know.

6. **Everyone should understand and comply with the law.**

   Every use of personal information must be lawful. The guidance above is drawn from Data Protection Act 1998 and guidance distributed by the Information Commissioners Office. We all have a duty to adhere to principles set out in the law.

Things to Avoid

- Don't mislead individuals about whether you intend to share their information.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is shared for.
- Sharing personal information when there is no need to do so.
- Not taking reasonable steps to ensure that information is accurate and up to date before you share it.
- Using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data.
- Having inappropriate security measures in place leading to loss or unauthorised disclosure of personal details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a fax machine.
- Sharing information with others that do not need to know that information.
- Accessing systems to get information when there is no intention to use or share information for work purposes.
- Sharing information with persons you do not know or have not been aware of previously in a working capacity unless you are absolutely sure they are who they say they are. For example people telephoning for information, staff should be aware there may be instances that others try to obtain information by deception.

If any doubt staff should speak to the Bridge Manager.