Appendix B

Ashford Borough Council

Data Security Breach Management Policy

1 Introduction

1.1 If a data security breach occurs this can have serious implications for Ashford Borough Council (referred to in this Policy as **Ashford**, **we, us or our**) and any individuals whose Personal Data (as defined below) may have been lost or accessed in an unauthorised manner.

1.2 This Data Security Breach Management Policy (**Policy**) explains the procedure that you should follow as soon as you become aware of a data security breach.

1.3 This Policy will help us ensure that the consequences of data security breaches are managed as quickly and effectively as possible and ensure compliance with our legal obligations, which may involve reporting data security breaches to the Information Commissioner and/or to affected individuals.

1.4 This Policy sets out the procedure which all Ashford employees and contractors (referred to in the remainder of this Policy collectively as **employees**) and all councillors must comply with if they become aware of a data security breach.

1.5 If you have any questions about this Policy, please raise them with Ashford's data protection office (**DPO**), Charlotte Hammersley, at any of the contact details below:

Email: charlotte.hammersley@ashford.gov.uk
Phone: 01233 330878
Address: Civic Centre, Tannery Lane, Ashford, Kent TN23 1PL

2 What is a data security breach?

2.1 A data security breach occurs if there is breach of security that leads to:

2.1.1 the accidental or unlawful destruction, loss or alteration of Personal Data; or

2.1.2 any unauthorised disclosure of or access to Personal Data.

2.2 For the purposes of this Policy, **Personal Data** includes information that is confidential to Ashford such as draft reports and legal advice and all personal information.

2.3 **Personal Data** includes any information about a colleague, a tenant, a member of the public or any other individual, including name, address, telephone number, bank details, health records and personnel records.

2.4 Examples of data security breaches include:

2.4.1 loss or theft of Personal Data or equipment on which Personal Data is stored;

2.4.2 inappropriate access or security controls allowing unauthorised use;

2.4.3 equipment or technical failure leading to loss of or corruption of Personal Data;

2.4.4 human error, for example sending an email to an incorrect recipient or forgetting to use the 'BCC' field instead of the 'CC' field;

2.4.5 hacking attack; or

2.4.6 "Blagging" offences where Personal Data is obtained by deceiving the organisation who holds it into believing the person requesting the information is entitled to access to the Personal Data.

2.5 A personal data breach can have serious consequences for the individuals concerned such as identity theft and fraud and it is important that each and every one of us takes responsibility for any potential, suspected, threatened or actual security breaches.

3 What do you do if there is a data security breach?

3.1 You must report **immediately** any potential, suspected, threatened or actual security breach to the DPO, who will ascertain the nature and severity of the breach.

3.2 You can use our Data Breach Reporting Form to report the breach. The Data Breach Reporting Form is available here. Please make sure you complete as much detail as possible before submitting the form to the DPO.

3.3 Your report should include the following details:

3.3.1 your name, job title and telephone and email contact details;

3.3.2 a description of what has happened;

3.3.3 when the breach occurred;

3.3.4 the volume of Personal Data involved and number of individuals affected;

3.3.5 the type(s) of data involved, including Personal Data and which individuals this affects;

3.3.6 status of the security breach, i.e. (i) potential (ii) suspected (iii) threatened (iv) actual (and if actual, has this been isolated (and how) or is it ongoing?);

3.3.7 whether the data security breach relates to a supplier arrangement and, if so, from where the security breach originated (i.e. from us or the supplier);

3.3.8 who is aware of the breach;

3.3.9 what actions have been taken to address the breach and have these mitigated any adverse effects;

3.3.10 any impacts caused as a result of the breach; and

3.3.11 any other relevant information.

4 Breach management procedure

4.1 The DPO will be responsible for co-ordinating the response to data security breaches with the support of the Breach Management Team. The Breach Management Team includes representatives from other services including Finance; HR, Communications and Technology; Legal and Democratic; Policy and Performance; Environmental and Customer Services; board member.

4.2 The Breach Management Team shall:

4.2.1 investigate the reported breach to establish the scale and nature of the breach;

4.2.2 consider what can be done to recover the loss of Personal Data;

4.2.3 identify the safeguards in place, or to be put in place, to protect the misuse of the Personal Data;

4.2.4 identify any relevant departments to assist and if appropriate, any third parties, such as banks, websites, insurers, police or credit card companies to prevent fraudulent use of Personal Data;

4.2.5 if the data security breach relates to supplier agreement, liaise with the relevant supplier in accordance with the terms of the relevant agreement;

4.2.6 by establishing the cause, determine whether any further actions can be taken to contain the breach e.g. taking systems offline, changing access codes, finding lost equipment etc.;

4.2.7 where the breach relates to unauthorised access or disclosure, determine the value of the Personal Data to the third party in receipt; and

4.2.8 take all necessary steps to mitigate the effects of the Personal Data breach.

4.3 The DPO will act as a contact point for the business and the affected individuals, and lead the co-ordination of remedial action.

5 Breach reporting

5.1 In some circumstances it will be necessary to report data security breaches involving Personal Data, including but not limited to, to the Information Commissioner. It may also be necessary to notify individuals of a data security breach if the personal data is particularly sensitive or if individuals need to take steps to protect themselves against potential misuse of their Personal Data.

5.2 The DPO shall be responsible for determining whether a data security breach needs to be reported to regulators, including but not limited to, the Information Commissioner or whether affected individuals need to be notified.

5.3 In order to evaluate whether a data security breach needs to be reported to the Information Commissioner or whether individuals need to be notified of the breach, the DPO shall take account of all relevant regulatory guidance and shall evaluate the likely risk to individuals. The DPO should consider factors including the number of individuals affected, the nature of the Personal Data affected, including whether special categories of personal data were affected and the volume of Personal Data affected. When carrying out this evaluation the DPO shall consider whether there are any risks of:

5.3.1 identity theft or fraud;

5.3.2 financial loss;

5.3.3 reputation damage;

5.3.4 loss of confidentiality protected by professional secrecy; or

5.3.5 any significant economic or social disadvantage to the individual(s) concerned.

5.4 If a data security breach involves Personal Data that is being processed by Ashford on behalf of a third party, details of the data security breach may need to be notified to that third party. The DPO shall be responsible for determining which data security breaches need to be notified to third parties.

5.5 Where we conclude that a data security breach needs to be reported to the Information Commissioner, the notification shall include the following:

5.5.1 a description of the nature of the data security breach including the categories and approximate number of data subjects and personal data records concerned;

5.5.2 details including the name and contact details of the point of contact where more information can be collected;

5.5.3 a description of the likely consequences of the data security breach; and

5.5.4 a description of the steps taken or proposed to be taken to address the data security breach and to mitigate any potential risks.

5.6 If we conclude that it is necessary to communicate the data security breach to the affected individuals, we will contact the individuals as soon as practicable. The notification will include the information noted above at 5.5.2-5.5.4 and provide individuals with advice on the steps that they can take to protect their position (if applicable).

5.7 Please note that should the DPO determine that it is necessary to notify the Information Commissioner of the data security breach, **the notification must take place within 72 hours of anyone within Ashford becoming aware of the breach**. Therefore, it is imperative that you follow through the process in the policy **immediately**.

6 Post breach review

6.1 After the event of a data security breach, the Breach Management Team shall evaluate the data security breach and the response to the breach and shall prepare a report for the DPO. The report shall:

6.1.1 summarise the data security breach event;

6.1.2 outline the steps taken in accordance with this Policy;

6.1.3 describe the effects of the data security breach;

6.1.4 detail the measures taken by the business to prevent similar breaches happening again; and

6.1.5 set out recommendation for any additional preventative steps that can be taken, including measures to improve the breach management response.

6.2 The DPO shall consider the content of the post breach report and shall determine what (if any) additional steps should be taken.

7 Data security breach log

7.1 The DPO shall record details of all reported data security breaches in a data security breach log. The log must include details of the nature of the data security breach, an assessment of the severity of the breach and the potential impact on individuals, whether the breach has been reported to the regulators (and if not, the reasons why it is not necessary to report to the regulators) and the current status of the breach.

8 Policy updates

8.1 We will review this Policy periodically and will make any updates it deems necessary. You will be required to comply with any updates made as from the date the updated Policy is made available to employees. We will let you know if and when any updates are made.

8.2 This Policy was last updated on 24/05/18.