Appendix 2

Tewkesbury Borough Council
Personal Data Investigation Guidance Notes
October 2013

There is no legal obligation on the council as a data controller to report breaches of security which result in the loss, release, corruption of personal data. The council, does, however, need to consider whether to notify those persons whose data has been lost, released or corrupted and/or whether to notify the Information Commissioners Office (ICO).

Although not an exhaustive list when assessing what action should be taken following a data security breach you (in consultation with One Legal) will need to consider the following:-

	Matters to consider	**Response**
	General points	
1	What has happened?	
	Type of data	**If the breach involves sensitive personal data relating to easily identifiable individuals, the greater the presumption will be that the data subject and the ICO are informed of the breach**
2	What type of data is involved?	
3	What is the volume of data involved?	

4	Are there any protections in place in relation to the data such as encryption?	
5	Is the information easily recoverable?	
6	Does the data relate to specific identifiable individuals?	
7	Does the detail contained in the data mean that an individual can be identified?	
8	If the information does not specifically indentify an individual what information does the data contain?	
9	Does the information allow a third party to build up a more detailed picture of an individual?	
10	Is the data that has been lost private information or information that is publically available elsewhere?	

11	How sensitive the data? Data will be sensitive if it is of a personal nature (i.e. information about racial or ethnic origin, political opinions or persuasion, religious beliefs or other beliefs of a similar nature, Trade Union membership or affiliation, physical or mental health or condition, sexual life, commissioned or alleged commission of offences, any proceedings for any offence, committed or alleged, including any sentencing decisions made by the court or sensitive because of what might happen if misused for example could be used for fraud or to assess financial information or accounts etc.)	
	Risk to the data subjects	**The greater risk to the data subject the greater the presumption should be that the data subject and the ICO should be informed.**
12	Who are the individuals whose data has been breached?	
13	What has happened to the data?	
14	Has the loss been contained?	

15	Is the data in a form that could be easily replicated or passed onto other third parties?	
16	Is the data in a form that could be copied and misused i.e. electronic signatures?	
17	What harm could come to those individuals? Could they suffer financial loss, reputational risks, risk to their physical safety?	
18	Would notification of the breach assist the individuals to mitigate any potential risk or harm?	

If you, in consultation with One Legal, decide to report the breach to the data subjects, they should be informed of what has been lost, the circumstances surrounding the loss, any steps they should take to mitigate the loss and a contact name at the council who can deal with queries regarding the loss.

If you, in consultation with One Legal, decide to report the breach to the ICO, One Legal will assist with the process.

You may also want to consider:-

- Any weak points in existing security measures that lead to the loss of data on this occasion.
- Are sufficient measures in place in relation to the security and retention of material of data?
- Revisit whether the training is sufficient