Recovery Plan Template

All fields must be completed:

Name and Number of Performance Indicator/Risk: RECPI07 Number of Data Breaches	
Definition of indicator/Background information: (Include current performance)	
Data breaches occur in the following instances relating to personal and sensitive information: • Loss • Inappropriate / unauthorised disclosure of information • Unauthorised access to information • Unauthorised destruction of information Examples can include: • Leaving a notebook with case notes in a meeting room / cafe / train • Sending a council tax bill to the wrong person • Telling someone who is not authorised to know information about someone else without that person's permission • Allowing a third party or unauthorised person to access information / a database • Looking up details of friends, family, neighbours out of interest • Sending an email to the wrong person, where it contains personal information • Loss of mobile devices such as iphones / ipads / PDAs which contain personal information • Throwing away paper records in a normal bin rather than confidential waste. The Council holds a significant amount of personal and sensitive information about our customers and staff and the potential impact of data breaches cannot be underestimated. Data breaches can potentially lead to damage and distress to an individual(s) in a number of ways. People can have their identities stolen leading to financial loss and there are areas of service where it is important for safeguarding reasons to ensure we are protecting personal data. The more information being processed by a department the greater the risk. In 2014/15 there were 23 data breach incidents reported across the Council. In the period April 2015 to February 2016 there have been 33 data breaches across the Council.	
Date of Recovery Plan:	March 2016
Why is this indicator/risk underperforming?	
It is difficult to know whether the increase between 2014/15 and 2015/2016 is due to a genuine increase in data breaches or whether it is due to staff being more aware of their responsibilities around data protection and the requirement to report breaches for an investigation to take place. Analysis of the breaches which have occurred over the last 10 months shows they have all been low risk and span across the Council.	

What actions are required to put this indicator/risk back on track?

- There are a number of information security policies already in place to protect information being stored electronically, these need to be reviewed.
- Data protection forms a part of staff induction even training.
- Staff and Councillors need to be reminded of their obligations under Data Protection Act, how to reduce the risk of a data breach and what to do in the event of a breach.
- Targeted training on processing information needs to happen across departments where there are higher risks.
- A regular review of the recommendations from data breach investigations takes place to ensure that they are being implemented.

Key Actions to be taken:	**Milestones (Dates):**	**Officer Responsible:**
Review of all 15 information security policies	March 2017	Jo Beer – Information Security Group
Regular staff communication on data protection	On-going	Jo Beer
Deliver training through induction events	On-going	Jo Beer / Information Compliance Team
Identify high risk areas for targeted training	June 2016	Jo Beer / Information Compliance Team
Deliver targeted training for high risk areas	March 2017	Jo Beer / Information Compliance Team
Regularly review recommendations from investigation reports.	On-going	Jo Beer / Information Compliance Team
Approved by Director/Executive Head:	Yes/No	
Approved by SLT	Yes/No	