DATA SECURITY BREACH
REPORT AND RECOMMENDATIONS
March 31, 2017

1. Introduction

The Chief Executive asked me to investigate the data security breach that led to the email addresses of more than 500 people potentially being accessible on the council's website for a time during 17-18 March 2017. The breach has been the subject of complaint to the council by twenty individuals. At the Chief Executive's request, I notified the breach to the Information Commissioner's Office on Monday March 20th 2017.

This report is made to the council's management team. It describes the breach and its consequences, how it happened and makes recommendations as to how similar breaches can be avoided in the future.

I have looked at all of the complaints, but particularly that made by AB. AB appears to have been the first person to discover the breach. He set out his concerns in a structured and detailed way that has been useful in writing this report. I have interviewed Fylde officers CD and EF, as well as AB. I am satisfied that this has given me sufficient information to understand how the breach happened and to make recommendations to avoid similar breaches.

I have used the following acronyms and abbreviations:

DPA: Data Protection Act 1998

EEA: European Economic Area

ICO: Information Commissioner's Office

PSPO: Public Space Protection Order

All names have been anonymised in this report. The initials used to refer to individuals are not their own initials, and the genders by which individuals are referred to are not necessarily their own.

2. Context

The context of the breach was a consultation by the council about the possibility of making PSPOs relating to dog controls in various parts of the borough. PSPOs are a new statutory mechanism introduced under the Anti-Social Behaviour, Crime and Policing Act 2014. No PSPOs presently exist in the borough. The proposed PSPOs would replace a number of existing byelaws and other regulations in relation to dogs, but would in some cases impose additional restrictions.

The council consulted widely on the PSPO proposals, which generated a great deal of public interest and engagement. The channels of consultation included a survey through Survey Monkey, accessible via the

council's website. The survey comprised a number of questions that respondents were required to answer by ticking responses. It also gave respondents the opportunity to add free text comments and invited them (but did not require them) to give their email addresses. Respondents were assured that their email addresses would not be disclosed or shared with any other person. The survey generated 1996 responses, of whom 948 left comments in the free text box and 586 left email addresses.

3. What happened?

Email addresses

Email addresses of individuals could be viewed via the council's website. This was a data protection breach.

The breach was the provision of a link from the council's website to unredacted survey results data on the Survey Monkey website. The link was put up on the council's website at 14:37 on Friday 17 March and taken down at 18:05 on Saturday 18 March. During that time, visitors to the relevant page on the council's website could, via the link, view all data gathered in the survey, including email addresses of respondents who had left email addresses[1]. Email addresses could be seen by inspecting the responses to question 35 (which was the question requesting respondents to leave their email address) and at the foot of individual responses to other questions.

Email addresses are personal data. Publishing them (including making them available through a link to a website) is a form of processing. Processing personal data is regulated by the eight data protection principles set out in DPA. The first principle states that personal data '*shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 [of the act] is met*'.

None of the respondents consented to their email addresses being made public. In fact, respondents had been assured that their email addresses would not be shared. Making them available to the public in those circumstances was therefore not fair processing and was a breach of the first data protection principle.

The seventh data protection principle states that '*appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data*'. This principle is also engaged by the breach.'

IP addresses

The information accessible via the Survey Monkey link also included the IP addresses of all respondents. IP addresses are not personal data (as established by a number of Information Commissioner decisions,

[1] *Two of the respondents included other personal data, such as names or addresses, instead of email addresses. These are also personal data and the same principles apply to them.*

for example decision FER0530573, Hackney LBC, November 2014). The disclosure of the IP addresses was therefore not a data breach.

Transfer of data outside the EEA

The survey responses were stored on Survey Monkey's servers, which are outside the EEA. This was not a breach of DPA but may have been a breach of the council's own Data Assurance Policy.

The eighth data protection principle is that personal data must not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Survey Monkey's servers are in the United States, which is outside the EEA.

The European Commission has formally decided that the EU-US Privacy Shield provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. This means that personal data can be transferred to an organisation in the United States without the transferor being in breach of the eighth principle if the organisation receiving the data is certified under the EU-US Privacy Shield. Survey Monkey Inc. is certified under the Shield. The use of Survey Monkey is not therefore a breach of the eighth principle.

The council's data assurance policy seeks to reflect the data protection principles, but there is an ambiguity in relation to the eighth principle. The policy provides, at paragraph 4.4:

> *'You must only process personal data in accordance with the eight data protection principles. These are contained in the Data Protection Act and summarised here:*

Each principle is then set out, followed by a few lines of commentary. The eighth principle is dealt with in this way:

> ***'Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.***
>
> *'Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. You should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA'*

While the intention of the policy is clearly to require compliance with the eighth principle, the commentary is more restrictive, in that it does not contemplate transfers taking place to non-EEA countries, even where there is an adequate level of protection. The ambiguity is that this more stringent approach is at odds with the overarching mandate to process personal data in accordance with the eight data protection principles.

If the commentary is taken as qualifying and further restricting the eighth principle, then the use of Survey Monkey was in breach of the council's policy (though not of the Data Protection Act).

There appears to have been no active consideration of whether or not the use of Survey Monkey would comply with the eighth principle or the council's policy.

4. How did it happen?

Data consisting of comments from respondents to the survey (left in the free text box) was originally posted on the council's website in the form of a PDF file. The PDF file had been generated from an Excel file containing data that had been downloaded from the Survey Monkey site and did not include email addresses. GH subsequently emailed EF and CD to say that there had been complaints from members of the public who had been unable to properly access their own responses to the consultation and those of others. This was due to the unwanted cropping of some of the data when the Excel file had been converted to a PDF.

The problem with the PDF file only applied to a very small number of responses. Nevertheless, EF uploaded the Excel file to the council's website, so that the data was available in the alternative formats of PDF and Excel. Neither of the formats contained email addresses.

Though the Excel spreadsheet contained all of the data, including data that had been cropped out in the PDF document, viewers had to click inside individual cells to access the full information contained in the cell. This had caused some viewers to contact the council to complain that the full information was not available.

The PSPO proposals attracted a lot of interest. Suggestions had been made that council officers were determined to introduce the proposed PSPOs and were prepared to improperly manipulate the consultation exercise and data to secure their adoption. Against this background, EF and CD were keen to respond to accusations of malpractice by demonstrating openness and transparency. Consequently, on the afternoon of Friday 17 March, they discussed ways of making the survey information fully available in a way that would remove any scope for mediation by the council by providing a direct link to the survey data on the Survey Monkey website. CD agreed to EF's suggestion and EF put in the link later that afternoon.

There were no written change management procedures that applied to the alteration of website content, the introduction of new content or the introduction of links from the council's website to external material. EF checked that the link they had made was working, but did not fully check that material accessed via the link did not contain personal information. EF has confirmed that he has been trained in data protection principles, and that he would have recognised the email addresses as personal information, and that they would not have been made available to the public if he had been conscious of them being accessible through the link. The email addresses could be viewed on the last of the seven pages that made up each response to the survey.

The link to Survey Monkey, including the availability of the email addresses, was available via the council's website from 14:37 on Friday 17 March until 18:05 on Saturday 18 March. It was then removed by EF following the complaint by AB, who had called the council's emergency number (manned at and by Progress Housing), and whose complaint had been passed through to the council's Chief Executive.

The removal of the link did not remove the entire problem, since the data, including the email addresses, was still available on the Survey Monkey website, and could have been accessed by anyone who had copied the link, or whose browser had cached it. The data was removed from Survey Monkey by 21:00 on 18 March, following correspondence between EF and Survey Monkey support staff. Again, AB had alerted the Chief Executive to the issue, and he had contacted EF by phone at approximately 20:30.

Neither the Chief Executive nor EF was at work or on call on Saturday 18 March.

5. Consequences

The direct consequence was that the Email addresses of 586 respondents to the survey may have entered the public domain. Because the email addresses were linked to survey responses, the views of the owners of the email addresses on the survey questions may also have entered the public domain. The indirect consequences could include the use of the addresses to send spam mail or the possibility of some survey responders being harassed or ridiculed because of their response.

42 hits were made on the Survey Monkey data from the time the link was posted until the time the data was removed. Three of the hits were by council officers, and one must have been by AB. This leaves 38 hits. It is impossible to know if any of the individuals who accessed the Survey Monkey data will use the email addresses for any purpose. The data may remain in their possession and could be passed on to third parties.

The council reported the breach to ICO on Monday March 20. If the Information Commissioner considers the breach to be serious, enforcement action could be taken against the council. This could include a financial penalty.

6. How could the breach have been avoided and what can be done going forward?

The decision to link to the raw survey data

The decision to provide direct access to the Survey Monkey data was discussed, decided on and implemented in a short time on a Friday afternoon. Only two officers were involved in the decision. The decision was taken in response to customer concerns about the accessibility of the data in the format in which it had been posted and in circumstances where the officers were trying to avoid giving the opportunity for further criticism of the council's approach to the consultation.

AB's critique points to a lack of change management procedures, or application of change management procedures, to sign off the addition of the Survey Monkey link to the council's website. It is true that a structured and documented approach to changes to the website, leading up to sign-off by a responsible

manager, may have avoided the breach. But this must be set against the need for responsiveness and agility. Under a more prescriptive approach, it would probably not have been possible to have had the change approved in time for the link to have been provided until the next working week. While that would have been preferable in this case, a general retreat to defensive decision-making would cut against the grain of the Fylde competencies and expected behaviours.

On the other hand, data protection breaches such as this must be avoided. There should be no perception that inadvertent disclosures of personal data are an inherent risk in the council's way of doing things. The next best thing to having a data protection specialist involved in decisions (or perhaps an even better thing) is to have decision makers become experts in the practical application of data protection. This would need an increase in practical training. The intention would be that managers and decision-makers not only know the principles of data protection, but understand how it applies in their everyday activities. There are a number of practical training resources available from the Information Commissioner, which could be used in-house. There are also a number of competent external training organisations that specialise in training in this area.

The data breach has been widely publicised, and there is a need to rebuild confidence in the organisation's ability to handle personal data appropriately. The first stage of doing this would be to carry out a self-assessment of the council's data protection compliance. At the same time, the Chief Executive will sign the Personal Information Promise. The Promise is intended to help strengthen public trust and confidence in the way organisations handle their personal information. It is a clear statement from the very top of an organisation that it values the personal information entrusted to it and will put the appropriate resources in place to look after it. It also sends a clear signal to the workers in the organisation about the importance of looking after people's personal information and that this is something that is taken very seriously at senior level.

Following the self-assessment, and after making any changes and improvements that flow from it, the council might consider asking for a data protection audit. These audits are carried out by the ICO, and provide an assessment of whether an organisation is following good data protection practice.

'Security, information risk and data protection' is a standing item on the agenda of the council's Strategic Risk Management Group. I recommend that a similar standing item be added to the agenda of the regular Management Team/Middle Managers meeting. As well as providing an opportunity for discussion of any relevant matters, the inclusion of the item would be a signal of the importance attached by senior management to full compliance with legal obligations and good practice in data management.

I do not recommend that any officer should be the subject of formal disciplinary action. A mistake was made, in that EF provided the link to Survey Monkey without fully checking whether the link made available any personal data. He meant to and should have checked this, but did not. However, in the absence of any documented instruction or procedure requiring to make such a check, it would be difficult to show a disciplinary breach. The officer has no disciplinary history, and in the light of what I would take

to be a positive attitude and contribution, it would seem contrary to the culture of the organisation to do so. The Chief Executive has made a commitment to provide support and advice.

The use of Survey Monkey

The possible breach of the council's own Data Assurance Policy, and the lack of reference to it reinforces the need for further training referred to above. But there is also a need to revisit the policy to remove the ambiguity by which the council's policy may be more restrictive than the eighth data protection principle requires.

So far as I know, there is no business or other reason why the council should restrict the overseas transfer of personal data beyond what is required for compliance with the eight data protection principle.

My further recommendation flowing from this element of the matter is therefore to amend the council's Data Assurance Policy to make it clear that it is permissible to transfer personal data to countries outside the EEA where an adequate level of protection is in place that would satisfy the eighth principle.

7. Summary of recommendations

- Improve data protection competence and understanding through a programme of training on the principle and practical application of data protection from the level of middle management upwards, with external facilitation to be considered.
- Reinforce confidence in the council as an organisation that is committed to protecting personal information by carrying out a self-assessment of DPA compliance with a view to inviting the ICO to carry out a Data Protection Audit, and by the Chief Executive signing the Personal Information Promise.
- Include a regular item about data protection on the agenda of the Management Team/Middle Managers meeting and continue to include it on the agenda of the Strategic Risk Management Group.
- Amend the council's Data Assurance Policy to make it clear that it is permissible to transfer personal data to countries outside the EEA where an adequate level of protection is in place that would satisfy the eighth data protection principle

Ian Curtis

Head of Governance

31 March 2017