ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.gov.uk

Mr Paul Funnell
IT and System Manager (Data Protection Officer)
Brecon Beacons National Park Authority
Plas y Ffynnon
Cambrian Way
Brecon
Powys LD3 7HP

27 March 2012

Case Reference Numbers ENF0424170 and ENF0433161

Dear Mr Funnell

Re: Self reported Security breach Incidents

Given the similar nature of the two security breaches reported by Brecon Beacons national Park Authority (the Authority) recently, the Enforcement Department has decided to deal with these cases together, in consideration of any Enforcement action.

ENF0424170 (PDF copies of comment forms re LDP)

In response to your email of 14 November 2011 concerning the unauthorised disclosure of personal data, held in 420 local development plan consultation comments forms, on your organisation's website, I would make the following points.

From the information provided it appears that this personal data is of relatively low sensitivity being email addresses, phone numbers and signatures. An unspecified number of these details related to organisations as well as to private individuals. Its disclosure would appear to be unlikely to cause significant detriment to the individuals concerned, if compromised. I note that the server logs show access to the documents was limited to staff and automated search indexers from Google, Yahoo and Yandex only.

As you are aware the Data Protection Act 1998 requires that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Act states that "Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level

of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful

processing or accidental loss, destruction or damage as are mentioned in the seventh principle,

and

(b) the nature of the data to be protected."

The measures taken should be in proportion to the detriment that could be caused to the data subjects if their personal data were to be compromised. This will obviously depend on the nature of the information involved.

The remedial measures you have outlined appear proportionate to the detriment that may be caused to the data subjects. However, the Authority may also wish to consider my comments below on access to the documents by automated search indexers, to ensure compliance.

You also ask for advice about whether to write to all respondents again regarding the inaccuracies in:

1. the dates of publication (presumably the 27th September 2011 quoted incorrectly instead of 28th); and
2. the date by which the responses would be put back in the public domain (presumably 8th December quoted incorrectly instead of 8th November 2011).

Matters of this nature fall within the responsibilities placed upon data controller organisations. Where an issue is of a sufficiently serious nature such a decision should be taken at an appropriately senior level within that organisation. In this instance consideration should be given as to whether the above two inaccuracies are serious or significant enough, in terms of any potential detriment to data subjects, to merit a correction of the type you outline. That said, organisations often take proactive corrective action of this nature from a purely "good practice" point of view.

It would appear, from the information provided by you that the second inaccuracy point has been answered to a certain extent by events, given that the date is now 27.3.12 and a correction was also previously placed on your website. It is not entirely clear to me why a correction regarding one

inaccuracy was published on your website but the other inaccuracy was not.

With regard to your server logs showing access to the documents being limited to staff and automated search indexers from Google, Yahoo and Yandex only, I

would make the following points. If there are no other visits to the pages in question then your web site operators can be fairly confident that no other persons requested the pages (assuming your web server is set-up to log every request).

However, both Yahoo and Google store copies of the pages they visit in a cache. When a result is returned from a Google search one has the option of visiting the live page or a copy of that page as it was when Google visited and indexed it. At the end of each search result is a cached link, which is a link to a copy of the page on Google's servers. If an individual visits this then your organisation would have no idea that they did so.

As such, your organisation's website operator would need to make sure that the search engine's cache is clear. A tool to request the removal of pages should be offered by the search engines.

This case has been taken into consideration when considering what Enforcement action is appropriate regarding the more serious incident outlined below.

I turn now to the more recent security breach case regarding the unauthorised disclosure of an estimated 70,000 copies of documents relating to planning applications which hold personal data of members of the public dating back to 2008.

ENF0433161

I write further to my email to you of 1 February 2012 which confirmed receipt of your report regarding the latest self reported security breach incident at the Authority.

For the sake of clarity, it is my understanding that on 13 January 2012 a member of the public brought to the Authority's attention an unauthorised disclosure of personal data on the Authority's website relating to planning applications. Copies of planning application documents which included personal email addresses, phone numbers and signatures of members of the public were published on the Authority's web based document management system.

Although the disclosed documents constituted part of the public record of the

planning file, the PARSOL rules for digital publication were not followed and therefore the publication of these documents was in breach of the Authority's Data Protection Policy.

The documents containing the personal data have been available on the web system since its introduction in 2008, or their later submission and upload.

Information regarding over 18,000 applications is available. You approximate that of the total number of published documents, which is estimated at 280,000, a quarter or 70,000 documents, may contain some form of personal information.

The Seventh Principle of the Data Protection Act 1998 (the Act) states:

"Appropriate technical and organisational measures shall be taken against the unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data."

The Authority should have taken steps to ensure that the disclosed personal data had been redacted for digital publication and thereby complied with its own Data Protection Policy.

Although the personal data in question here is again of a relatively low sensitivity, being email addresses, phone numbers and signatures of members of the public, it is noted that a potentially large number of individuals have been affected by this disclosure.

On the basis of the information provided, it would appear that the Authority has not taken adequate steps to prevent the unauthorised processing of the personal data. In our view the Authority has breached the Seventh Principle of the Act.

We welcome the various remedial steps taken by the Authority, as outlined within the report provided to this office. In light of the steps taken to date, we are satisfied that it is not necessary for us to take any formal enforcement action at this stage, subject to the Chief Executive for the Authority agreeing to an undertaking (attached) which details the steps that the Commissioner expects to be taken in order to mitigate similar incidents in the future. Consideration will be given to any representations, should the Authority wish to alter the terms of the Undertaking, otherwise the Undertaking should be signed and returned to this office.

You will note that as long as the Authority implements the measures detailed in the report provided, it will be complying with the terms of the undertaking.

Information Commissioner's Office

Please be aware that any undertaking signed by the Authority will be published on our website, and we may issue an accompanying press release. Furthermore, if the Authority were to sign this undertaking and subsequently breach its terms, it is likely that we would take formal enforcement action against the Authority.

I would appreciate confirmation as to whether the Authority is prepared to agree to this undertaking within **14 days**.

Please contact me on 01625 545838 if you wish to discuss this matter.

Yours sincerely

[redacted]

Andrew Allan
Case Officer – Enforcement
Information Commissioner's Office
Direct dial number: 01625 545838