Web Strategy Group
8th December 2014
14.00 IF4.02

AGENDA

1 – Update and Timescales on Migration from Polopoly to Drupal [K.Bell]

2 – Update on Internal Web Site [K Bell]

3 - Front Page Freshness [K Bell]

4 – Data Protection Breach & Follow Up (PAPER A) –[S Scott]

5 – Website Edit Permissions - CVS [T Totterdell]

6 – Better Informatics / PATH – Update [M. Rovatsos]

7 - Research Pages in Polopoly [T. Totterdell/M. Fourman]

8 – Any Other Business

Data Protection on the Informatics Website

Background:

This issue came to light on the 20th November 2014. During email correspondence with IS and Records Management discussing the possible wording of a web banner disclaimer, we were asked to provide a sample of old pages we were looking to target. Some of the pages we provided were student lists for tutorials and courses. They informed us that the external publication of student names without explicit consent from the students was a breach of data protection and that we should remove all pages with this type of content immediately.

Initial Breach:

We identified 25 pages which were in breach of data protection and we set up redirects to remove them from public access. We also contacted Google and these pages have been removed from search results. We followed university guidelines and completed a Data Protection Breach Evaluation Form and provided Records Management with copies of the information in question. We met with Susan Graham the University Records Manager to discuss in more detail data protection on the web and how we could take things forward.

How do we locate other pages which breach the DPA?

Although we have dealt with this initial breach which was involving pages within Admin/ITO, we have since identified other pages which breach DPA regulations in other areas, these lie in Teaching, Staff homepages, Student Homepages, Institute Sites and student-services plone.

Proposal

To find absolutely everything, a manual search could be done but this would be very resource intensive. It may be possible with the help of support to set up an automated search which will look for sensitive data but we do not know how effective this search will and it's unlikely to find all possibly sensitive data. Regardless of how much data is returned by the search, we have no way of knowing this is complete. We could also use different tactics for different sections:

School CVS

Either:

1. Move all School CVS pages (other than /teaching/courses) to a restricted area and go through as and when time allows to migrate to new CMS. Go through /teaching/courses (or ask academic staff to do so?) and deal with any breaches. OR
2. Target likely areas for breaches and trawl through to pull any pages that breach DP. Then go through rest as and when time permits. OR
3. Go through everything in the School CVS and pull any pages that breach DP. This option is extremely resource heavy, but for admin and computing staff.

School Services Plone

- Check pages manually – unlikely to be any issues here.

Student Services Plone

- Potential issues with reps - go through and ask for consent/check if it was given.

Institute Sites

- Ask Institute Directors to take responsibility for these pages and removing anything that breaches DP.

Staff Homepages

- Email to staff and ask Institute Directors to bring up at institute meetings. Responsibility to remove DP breaches lies with each individual staff member.

Student Homepages

- Probably more of an IGS issue than ITO - ask HoGs to mail students reminding them of policy.

Staff Details

- Staff details also breach data protection unless permission has been given. We plan to send out an email in the new year which will ask staff to confirm their details on the online directory. The email will also include information on opt-out procedures.

Photographs

- Many of the photographs we have published at Informatics events also breach DP. We need to think about how we cover ourselves at events like graduations. A disclaimer should be part of any email invite to anyone who may attend an event where photographs will end up being used by us online or in print.

Going Forward

In order to reduce the likelihood of future breaches we need to raise the awareness of DP across the School especially in relation to web publishing. We should also look at the creation and implementation of processes which ensure DP regulations are adhered to. In addition, we should also create local policy on web publishing permissions, content, style guides and also a process or cycle to ensure these are kept up to date.