A quick GDPR audit check!

a. Have you…..

1   Provided a Privacy Policy on your website

2   Added a GDPR statement to your admissions documents

3   Noted Satswana as your DPO on your website

4   Started a Processor list (see Guide, Appendix D!) (On the website under Resources)

5   Encrypted data wherever possible

6   Considered your retention policy (See below!)

7   Shredded all redundant paper records

8   Planned a response to a breach (Also below)

b. Ensured that Staff have an understanding as follows:-

1   That ownership of data is returned to the individual, together with a right to compensation and a right to be forgotten

2   That they are "not the target" when controlling data, so they should have no fear reporting a breach, even if an accident and/or embarrassing. (It is the cover up that gets you, not the breach.)

3   That work processes will change over the next few years to reduce paper files and favour digital document collaboration.

4   That data should be encrypted, especially where phones are used.

c. Are there any areas of doubt that we can help you with? We are always happy to visit, answer questions by email or discuss on the phone.

Retention Policy?

We will have discussed the benefits of deleting data as soon as you possibly can within the landscape that is coloured by Subject Access Requests and the Freedom of Information Act, but there is huge confusion as to what is actually the law, and what is custom and practice that can be changed.

Currently under review is the Information Management Toolkit for Schools produced by the Information and Records Management Society https://irms.org.uk/? And Satswana have sought to contribute to its production. In the meantime V5 dated 2016 is available here https://cdn.ymaws.com/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

It is written with regard to the DPA 1998 rather than GDPR but still has valuable information, though its concentration on a paper file is something we would wish to see radically changed in the next version. We hope to bring you an update as soon as it is published.

Concentrate the mind time? "Be aware that anything you write in an email could potentially be made public!"

E-mail applications are not designed for keeping e-mail as a record. E-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files. They can then be safely deleted.

Breach (and possibly Disaster) planning?

This is such an easy subject to lose sight of when all is going well, and a tragedy if it is not addressed and something goes wrong. We would like to highlight it in this update notice and ask you to take positive action as follows:-

a. Review all your backup policies for all your data systems and ensure that they are not only being conducted, but that you can also "restore" from them.

b. One of the risks you face is from Ransomware that will encrypt your data (even if it is already encrypted) which makes it inaccessible and unusable. If you do not discover this quickly enough, it can also infect your backups. We advise that once a month you take an "Archive" copy onto an entirely different server location. This then becomes a 'protected' backup that can also be an emergency data source. It cannot be ideal, as you may lose up to one month's updates to the system, but it is a lot better than having no data at all.

c. You must have a management response plan in place in case of a breach, with two essentials. First, a person both nominated and trained to handle the media or any external party with a prepared response script. Secondly a web page that you can instantly mount to inform online queries. (Ask us for help on this if you are uncertain how to go about it.) This must be planned for; you do not have a hope of getting it right by 'winging it'. (Do you recall the chaotic Talk Talk media circus?)

d. It can be disaster as well as a breach that compromises your data; both fire and flood would be a problem for paper records. That is yet another case for digitization where you can send the backup to a remote location.

We know that this is yet another job on a list that seems endless, but ask yourself what if it did happen, and you had not done it? Sorry to nag, but we think it important!