Satswana

Company registered number 09329065 www.satswana.com

The ICO Inspection

If the ICO turn up on your doorstep tomorrow morning on a snap inspection, what can you expect? Thanks to a most helpful contributor on the FD Forum we know what happened in one School, and we reproduce it here, with Satswana comments as appropriate!

1 They started with a tour of the School.

a) Security of access to the building. (In this example they tail gated in!)
b) Whether ID's are worn
c) Checked the information displayed on the walls
d) Did the windows have restrictors?
e) Were screens visible through the windows?
f) Was a clear desk policy in place?
g) Where are the keys kept?
h) Where filing cabinets were in the room, were they locked?
i) Is post left in the tray overnight?
j) Is the shredder a cross cut and what happens to the residue afterwards?

Satswana. Candidly we were surprised by (and learned from) their concentration on the physical security aspects. In the concentration on data that is easy to forget.

2 Security

a) Does support staff have GDPR training?
b) And outside agencies such as cleaners?
c) Do you spot check for clear desks and locked screens?
d) They recommend changing screen lock time from 30 minutes to 15 minutes for admin staff.
e) Laptops and USB's should be encrypted
f) Keep separate copies of USB data on the network – if lost. Lost USB's must be recorded as security incidents.
g) Lock down USB ports on computers
h) Do not take USB's home
i) Staff should not bring in their own devices, ICO BYOD policy on website
j) Update Mobile and Home working policy to encourage data protection in a home environment, for example – close windows, screen not on show to family, passwords. No student data on home computer. Any device taken out of school to be covered by policy
k) Home working should encourage use of school email and remote access
l) Update AUP – if required, school can view your network area and school email. School email should be separate from personal email
m) Asked to see a copy of AUP
n) Do you exercise your right to inspect your data providers? Record the evidence

Satswana. There are conflicts here, and different schools will read the comments differently depending on their state of adoption of change. It is an absolute that no USB stick should be unencrypted, but the practical reality is that they are used to take files home, thus will be subject to change, and the backup provisions then become unenforceable in a real world. The future is full use of a collaborative environment such as Microsoft 365 or Google Cloud, with minimal use of email – but necessarily on what may well be their own device (a phone). Only then can you ban USB's altogether and lock down the ports on PC's. We take note of the identification of support staff and cleaners as requiring training. The toughest nut is point 'n' – see our advice on Processors in Appendix D of our Guide.

3 Records Management

a) Asked the SBM what her role was
b) Asked about her history and background in school/work etc.
c) Have staff been issued with privacy notices and asked to complete consent forms?
d) Does the school refresh personal data (e.g. addresses, phone numbers etc.) every year?
e) Do they keep a note of personal files that leave the school such as student records?
f) Asked to see their data retention policy
g) How do we keep a record of what needs to be disposed of and when?
h) Do we do a sweep of files on a regular basis?
i) How we dispose, who do we use, where do they shred? (On or off site?)
j) Do we keep a central record of what has been destroyed?
k) Where are student files kept?
l) Who has access?

Satswana. We are all waiting for revised IRMS guidance on retention, and most schools have only really started to consider the challenges of data deletion since GDPR declared it to be desirable. The future direction is a single instance of data, held digitally, and its management largely automated. That is a huge change from historical practice, and will take time to implement.

4 Training

a) Who led it?
b) Who received training?
c) Content?
d) Have you checked that your staff understand it?
e) What materials were used to deliver it?
f) Any follow ups?
g) How will you ensure staff stay up to date?

Satswana. Whilst we must take anything the Regulator requires very seriously, we sense our customers will read this with a certain weariness. There is just so much training that you are expected to adopt, and here is another subject. Furthermore, at an executive level we are only just coming to terms with what is required, and perhaps we have not implemented the changes that we must before training is provided in the new procedures. As to staff understanding, do we fully understand it ourselves? However, it is clear that the profile of the topic has to be raised higher than it possibly is currently.

5 Subject Access Requests

a) What are they; do staff know what they are?
b) How do we manage them?
c) Do staff know what to do with them and who to go to?
d) Procedure for responding?
e) Is there a central record?

Satswana. A concentration on process, please see our document on SAR's under the Resources tab at www.satswana.com. We believe the University of Worcester decision commented on there is materially important 'case law' that will inform the future.

6 What they did not identify

The commentator remarked that nothing was asked regarding data breaches or supplier compliance, though in fact all contracts had been updated. Also they did not ask about CCTV other than commenting that they noticed it on the tour. They asked how the SBM was qualified to be the DPO.

Satswana. Different inspectors are going to have different priorities, and they only have so much time to address issues, so this cannot be taken as any sort of absolute guide. However, if "forewarned is forearmed" it is useful information, and suggests that both physical security and training have to be considered more strongly. Lessons will be learned and applied!