**GDPR information**

**shared with the South Regional Network**

**by Gloucestershire & Wiltshire partnership**

There is also some really useful information on the Information Commissioner’s website including information specific to education.

The main page is <https://ico.org.uk/for-organisations/education/>, and there are some FAQs at <https://ico.org.uk/for-organisations/education/education-gdpr-faqs>.  It does look rather onerous, but the workshop facilitators were keen to point out that the main difference between current data protection regulations and GDPR is that under GDPR organisations must be able to demonstrate compliance.  So in theory you should all already be meeting the data protection regulations, and so should be able to demonstrate compliance.

Below are some of the points I picked up:

* All staff should have regular data protection training -  however this can be as simple as showing an ICO video. There are a number of videos at <https://ico.org.uk/for-organisations/resources-and-support/training-videos/> and the page also signposts you to YouTube and Vimeo channels with videos.
* GDPR will be in  place 25 May 2018.   The ICO does not expect organisations to be fully compliant on this date but at least have formal plans in place to implement GDPR.
* The fines can be quite substantial.
* You need to state on a Privacy Notice why the organisation is collecting the data.
* Check personal information is up to date regularly and don’t keep data longer than is necessary.  It is a good idea to have a retention schedule for keeping data.
* Check whether your server is outside of EU?  If it is, change it.  As this is EU law, then all of the EU is covered under GDPR but this is not the case outside of the EU.
* Check your contracting arrangements if personal data is involved.
* The ICO will actively seek compensation for anyone who has had their data breached.
* You may need to review all of your policies ASAP.
* There are additional child consent considerations.  It will be aged 16 and above but in the UK, it may be age 13 and above.
* GDPR applies to learners, staff,  governing bodies, trustees, directors and anyone associated with your organisation for whom you keep personal data.
* You will need to report breaches within 72 hours and it is good practice to put a process in place to manage reporting.
* You will need to do Privacy Impact  Assessments before any new processes, contracts, purchases etc.
* There are self-assessments for data controllers and data processors available at <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/>.
* They said that as you wouldn’t hold personal data about employers, you shouldn’t need to note GDPR but I would double check this as I have heard differently.
* You will need to have a Data Protection Officer, but you can share one between organisations.
* Make sure you know where your idata informtion is held and that it is held securely.  You can decide what is ‘secure’ but there will need to be an evidence trail for how you made that decision.
* The ’12 steps’ I handed out at the meeting can be found at <https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf>.
* Don’t forget you also need to think about CCTV and photos.   You may want to review your retention policy for CCTV in particular – if someone asks for CCTV records and you have records over a period of time and would have to black out everyone in the video apart from the requestor, this will take a huge amount of time.  They talked about a request for playtime CCTV and this was 10 minutes, 25 photos per minute, over 3 months and imagine having to blur out everyone in each of those photos.
* Check with your local authority if they have an Information Governance Officer as they may be able to help you with queries.
* Risk assess your processes.