**GDPR (General Data Protection Regulation) – Notes From Training on 13 March 2018**

**(written by J Frew)**

Also see presentation from training (held on GVO/BFC School Management website/shared with SBM). It includes:

* links to further help such as the ICO (Information Commissioners Office) who advise on GDPR
* link to London Grid for Learning sample audit form – to do a data audit
* links to self-assessment tools

Intro

GDPR applies from 25 May 2018. Most schools/businesses will not yet be compliant. If they have a note on their website confirming compliance, they can be assumed to be compliant. Guidance is continuing to be updated.

The ICO is an independent body that upholds regulations but also advises and promotes good practice.

Data referred to is personal data, i.e. “any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

In addition, there are “special categories of personal data” that are more sensitive, e.g. ethnicity, religious or political beliefs, sexual preference, trade union membership, medical records, biometric data (fingerprints, eye scan etc).

What Does GDPR Require in Terms of Personal Data?

* Data has to be processed lawfully, fairly and in a transparent manner
* Data to be collected for specified, explicit and legitimate purposes
* Adequate, relevant and limited to what is necessary
* Accurate and kept up-to-date
* Kept in a form which permits identification of data subjects for no longer than is necessary
* Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

Implications for Schools

* Same basic principles as current DPA (Data Protection Act), but strengthened
* Greater accountability for data controllers, i.e. schools
* Increased rights for data subjects, i.e. parents and children
* Increased requirement to be able to demonstrate compliance
* New requirements for breach reporting
* Use of Data Protection Impact Assessments (DPIAs)
* Higher penalties for non-compliance

First Steps for Schools

* Establish GDPR ‘team’ in school to review and ensure document compliance
* Do an audit of data and processes
* Review privacy notice, data collection process, lawful basis
* Obtain positive consent where necessary
* Review data protection policies, update staff education
* Establish and record GDPR compliance of 3rd party processors
* Review physical and electronic security policy and processes
* Update process for SARs (subject access requests), FOI (Freedom of Information), data breaches, new projects, data deleting/retention
* Appoint Data Protection Officer (DPO)

Data Protection Officer

* DPO informs and advises, monitors compliance, trains staff, conducts internal audits, is the first point of contact on GDPR
* DPO must report to the highest management level, be allowed to fulfil their role (resources/training), operate independently and not penalised for carrying out their tasks
* There is conflicting advice about who to appoint as DPO; it is about making a reasoned choice and being aware of conflicts of interest
* In practice, most staff who would be suitable as DPO have some conflict of interest because they also process data (teachers, office staff, SMB, clerk)
* Trainer recommends that DPO is not an IT manager (too conflicting), or a governor (volunteer and would need to be available in emergency, e.g. data breach to advise/implement procedures). However if a governor has strong knowledge, they can be involved in the preparation process.
* Schools can share a DPO or appoint each other’s staff member to be the DPO. They can also conduct checks/audits for each other as they do on finance.

Additional – Establish Security (in relation to personally identifiable data)

* Secure emails
* Individual and strong passwords
* Encrypted USB sticks/drives/computers/mobiles, malware
* Secure printing
* Clear policies for homeworking
* Paper file security
* Removing access immediately when staff/governors leave
* Secure device disposal

Governors to:

* Designate a link governor
* Monitor GDPR compliance
* Understand that this involves an increased workload for staff