**GENERAL DATA PROTECTION REGULATIONS (GDPR) from 25 May 2018**

The Data Protection Act 2017 Bill continues to progress through Parliament. The bulk of the Act will be the GDPR regulations. Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA). However, there are new elements and significant enhancements. Like the Data Protection Act 1998, the GDPR sets out principles rather than specific rules. Schools need to decide the best way to apply the principles for data management in their own contexts, and there is little published information available at the moment on the specific steps a school should take to comply. More guidance is expected before May 2018.

**So… what are we doing at The Alderton Infant School?**

**1. Tell key people the law is changing i.e. staff, governors, suppliers, parents and carers**

**2. Appoint a data protection officer**
It is likely that our school will share a DPO across the new Multi-Academy Trust.

**3. Carry out an information audit**
Clarify what personal data we hold, where it came from, and with whom we share it. Our governing board's working practices will need to be considered too. Think about:

- What documents governors have access to and whether these contain any personal data?
- How governors get access to these documents?
- Whether information is sent to personal email addresses?
- Whether governors take information off the school site?

Personal data may be stored in a wide range of places, including IT systems, laptops, personal devices, paper records, USB sticks or other portable storage devices, email accounts, and staff members' homes.

**4. Identify lawful basis for processing data**
Under the GDPR, there are 6 'lawful bases' (or reasons) that a school can use to justify why it needs to process data. We will most likely use public task as our lawful basis for most of our processing. This means that we need to process personal data to carry out our official functions in the public interest. We will look at the personal data we hold and identify which lawful basis/bases applies to how we process the data. Then, document this and update our privacy notices to explain our lawful basis/bases.

**5. Review privacy notices**

**6. Review data processing procedures**
Data processing procedures will need to cover the new requirements. The new rules say we:

- Can't charge for complying with a request (in most cases) and have a month to comply (or 3 months where the requests are complex or numerous, in which case we must explain to the individual why the extension is necessary within a month)
- Can refuse or charge for requests that are clearly unfounded or excessive, particularly if they are repetitive or ask for further copies of the same information
- Can refuse a request, but within a month must tell the individual why, and that they have the right to complain to the ICO
- Must verify the identity of the person making the request using "reasonable means"

**7. Review how we manage consent**
We will check that we seek, record and manage consent in accordance with the rules. There is a consultation around consent taking place at the moment.

**8. Check processes adequately protect children's data**

**9. Review Data Protection Policy**

**10. Review contracts with suppliers**

**11. Carry out data protection due diligence on any existing suppliers which hold personal data**