Item for Engagement Committee

Since 1998 the school (and all other organisations that collect personal data about individuals) have been subject to the provisions of the Data Protection Act but what you may not be aware of is that, from May 2018, we will also be subject to the provisions of the General Data Protection Regulation ("GDPR"). Not only that but, in the last Queen's Speech, the Government announced plans for new data protection rules in the UK. Quite what impact these will have is not known at present, but it is understood that these will replace the 1998 Act and run alongside the GDPR.

Therefore, I have been tasked with looking at the implications of the GDPR for the school and, as a bit of a background, I thought that I would remind you that, prior to the Data Protection 1998 (and its predecessor the Data Protection Act 1984) and with more and more organisations using computers to store and process personal information, there was a danger the information could be misused or get into the wrong hands. A number of concerns arose:

- Who could access this information?
- How accurate was the information?
- Could it be easily copied?
- Was it possible to store information about a person without the individual's knowledge or permission?
- Was a record kept of any changes made to information?

Therefore, because of these concerns, the **1998 Data Protection Act** was passed by Parliament to control the way information is handled and to give legal rights to people who have information stored about them.

The Act applies only to data which is held, or intended to be held, on computers or in an organised paper filing system and anyone holding personal data is legally obliged to comply with the Act, subject to some exemptions. The Act defines eight data protection principles ("the data principles") to ensure that information is processed lawfully and these are set out in Schedule 1 to the Act. They are that personal data will:

- Be obtained fairly and lawfully and will not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not be transferred outside the European Economic Area (EEA)

Basically, since that time, and probably when we have thought about it, we have complied with the Act or, at least, with the spirit of the Act.

However, the forthcoming GDPR sets out certain things that we need to be aware of, the most significant one being the addition, in Article 5(2), of the new "accountability principle". This principle requires organisations to demonstrate that they comply with the data principles and to do this we must:-

- Implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation;
    - Pseudonymisation (which I am sure that I don't need to tell you is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms);
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

We can also adhere to approved codes of conduct and/or certification schemes but, at the moment, none of these are in existence although a Working Party set up under Article 29 of the GDPR is working on guidance on certification.

The GDPR also says that, where appropriate, organisations must appoint a data protection officer ("DPO"). In our case this is not necessary although we must ensure that we have sufficient staff and skills to discharge our obligations under the GDPR. The DPO's minimum tasks are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, parents etc.).

The organisation must ensure that:

- The DPO reports to the highest management level of the organisation – i.e. board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPO's to meet their GDPR obligations.

As you can see from the above, there is quite a bit to do between now and May and one of things I am trying to do is to undertake an audit of what data we have, why we have it and where it is stored.

Alongside this I have updated the current Data Protection Policy and I attach this for members of the Committee to have a look at and comment on or suggest amendments. If you could this as quickly as possible please that would be good.