General Data Protection Regulation (GDPR) – Schools

In June and July 2019, Norfolk Audit Services carried out a thematic audit on the General Data Protection Regulation (GDPR). A sample of 11 maintained schools were visited.

The specific objective of the audit was: -

- To provide assurance that schools can adequately demonstrate they are complying with the GDPR and that a Data Protection Officer (DPO) has been designated to take responsibility for data protection compliance.

Our audit findings

The visits highlighted that all of the Schools had a designated DPO in place to take responsibility for data protection compliance at the School. Three schools had an internal DPO and eight had external providers, five of which were with the Data Protection Education provider.

At all eleven schools, senior staff were aware of their roles and responsibilities in relation to the GDPR and adequate training had been undertaken and cascaded to the wider staffing team.

All eleven schools had reviewed and updated their privacy notices for the GDPR and had a documented procedure in place for dealing with subject access requests and detecting, reporting and investigating personal data breaches.

Retention policies or a schedule were in place and records were being disposed of in line with these. Appropriate details and information regarding the GDPR is reported to governors.

The following findings are an overall summary of the areas that need strengthening, and are not representative of every School visited: -

- The Information Commissioner's Office (ICO) had not been provided with details of who the designated DPO was at the School.
- An information audit, or similar exercise, documenting and considering all personal data that is processed and held at the School, had not been completed. It is understood that the external DPO recommended waiting for the introduction of a new data processing tool, due to be launched in September 2019, which would assist in mapping data.
- The lawful basis for which all data is processed and held at the School had not been identified.
- No checks had been carried out to ascertain the reasons why third party suppliers hold and process the School's data, and whether these reasons were lawful.
- The process for the completion of Data Protection Impact Assessments (DPIA) is not documented and staff have not been subject to any training around how to complete a DPIA, or to ensure they understand the need to

consider a DPIA at the early stages of any plan involving personal data.
It was noted that the required staff at these schools do have an awareness of when a DPIA would need completing.

Recommendations

We recommend the above issues are considered by your School's Leadership Team, together with any proposed actions for improvements you need to make in relation to your School. Any issues and proposed actions should be presented to the relevant Governing Body Committee for approval and monitoring.