Information Security in NCC maintained schools

In January 2017 Norfolk Audit Services carried out an audit of controls in place for information security within schools. This work followed on from the Information Commissioners Office (ICO) audit of Norfolk County Council in October 2016. As schools are responsible for their own information security they were excluded from the ICO audit. Norfolk Audit Services review has been performed to obtain assurance that schools have acted on the points raised in the 2015 Management Information sheet (Number 1/15). Eleven schools were contacted by telephone and the Headteacher's or staff responsible for information security were asked a set of questions. The conclusions stated below have been based on the responses received.

Our audit findings

From the responses received it can be concluded there has been improvement in the information security arrangements in schools. These include the following in respect of all schools:

- A named officer is responsible for information security.
- Mechanisms are in place to ensure all staff, including volunteers and contracted staff, are aware of their responsibilities.
- Confidential information is held securely in locked cupboards and restricted access.
- Staff are fully aware that confidential emails sent to recipients outside school must be sent securely. Personal emails are not allowed to be used.

The areas needing further strengthening in some schools are:

- Where schools are placing reliance on the staff code of conduct, instead of Data Protection or Information Security policies, they need to ensure it is fit for purpose in respect of data protection, Caldicott principles and home working.
- Obtaining formal acknowledgement from staff that they understand their responsibilities in respect of information security.
- Better records of relevant training in respect of information security (including refresher training) to be maintained.
- Records to be maintained where pupil files are removed from the school to monitor usage and return.
- Ensure all electronic data is password protected.
- Ensure any IT equipment with confidential information is encrypted.
- Email usage to be monitored to ensure staff are complying with school expectations.

- Clear home working procedures in place including the use of IT equipment.
- Staff signing or agreeing to the terms of use for any electronic device issued to them.
- Records in place to evidence the issuing and returning of laptops and memory sticks.
- Clear guidance on how breaches of confidentiality are detected, investigated and reported.
- Lack of understanding of the risks to data security and how to assess and document them.
- A more robust process in place to identify exceptions and non compliance of procedures in respect of information security.

We recommend that the above issues are considered by each 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

A reminder that all schools are responsible for ensuring that the Data Protection Act 1998 and Caldicott Principles are complied with and must register their individual school with the Information Commissioner.