# Information Security in NCC maintained schools

From January 2014 we changed the way we work and carry out audits. The changes included carrying out themed audits, visiting a sample of schools and sharing any findings and examples of good practice with all schools. Earlier this year we carried out an Information Security audit in NCC maintained school. Our assurance work was completed with a small sample of schools by interview, examination of procedures and documentation and observation with representatives deemed by the school as responsible for information security. Our work found there to be an inconsistent understanding and approach to information security in schools.

## **Your** legal responsibility

Schools retain a large volume of personal and confidential information and data. All schools are required to ensure that the Data Protection Act 1998 and Caldicott Principles are complied with and must register their individual school with the Information Commissioner.

The Information Management Services within NCC offer support for schools, however it is the responsibility of the schools themselves to ensure all relevant policies are in place at the school, reviewed and approved by Governors, understood and complied with by all staff, including voluntary staff and contractors.

## Our audit findings

Our audit work within the schools visited focussed on the processes and documentation in place for information security. The following is an overall summary of the issues we found from the schools visited:

- Data Protection or Information Security Policies were not in place
- Staff were not aware of and understood their responsibilities regarding information security. There was no formal acknowledgement through either signing a code of conduct, recording that they have read the policies on an annual basis or by agreement on accessing the school's management information system.
- Records were not maintained to evidence training staff had undertaken in respect of information security.
- Access to personal paper documents is not always restricted and records not maintained where pupil files are removed from the school to monitor usage and return.
- Electronic data not kept in a secure environment and staff not aware of what is classified as ‘confidential’ data.

- Unencrypted devices and privately owned computers are used to transfer data.
- Schools not aware of how to prevent, discover, record, investigate and report information security breaches.
- No clear home working policy or procedure in place.
- Staff not signing or agreeing acceptance of terms of use for any electronic device issued to them.
- Records not maintained to evidence the issuing and returning of laptops and memory sticks.
- Users of school email systems had not signed an Acceptable Use Policy and email usage not monitored within schools.
- Lack of understanding of the risks to data security and how to assess and document these within schools.

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.

Further advice or guidance on Data Protection, Freedom of Information, Records Management, Data Sharing, Data Quality and Data Security, can be obtained from the Compliance Team, who are part of the Information Management Shared Service, and can be contacted by email on information.management@norfolk.gov.uk or by telephone on 01603 222661 or alternatively visit the Information Commissioner's Website at www.ico.org.uk.

## Useful policies and guidance

The following is a list of policies and documents which you can access via the Norfolk Schools website, under School Administration, Legal, Information Management. (http://www.schools.norfolk.gov.uk/School-administration/Legal/InformationManagement/index.htm).

Schools are responsible for their own information management. These policies are available to assist schools in formulating and agreeing their own information management policies. Whilst NCC makes every effort to ensure the accuracy and correctness of these policies we make no warranty or representation as to their content or fitness for purpose and you understand and agree that NCC will not be responsible for any claim, loss or damage resulting from their use.

- Information Security Policy - Corporate
- Information Security Policy for Employees
- Data Protection - an introduction to the Policy
- Data Protection - expanding on the Policy
- Breach Management Procedure
- Data Sharing Code of Practice (Information Commissioner's Office)
- Incident Management Process

- Email E-Diary Policies
- Safehaven Policy
- Confidentiality Policy and Code of Conduct

All policies and documents will need to be subject to regular reviews, approved by Governors and appropriate staff made aware of their existence.