Security Advice on Use of Cloud Storage and Transmission of Data

All Council, School and Academy employees have a legal requirement to maintain the confidentiality of information and personal data under the Data Protection Act.

Any documents that need to be sent outside the Council must therefore be protected if they contain sensitive or personal data, i.e. they must be encrypted. The Council has several recommended methods of transmitting sensitive data including:

- GCSX secure email, where data is passed over a private network
- 7-Zip file encryption for securing data passing over public networks
- VPN – for site to site encrypted data transfer over public networks
- Encrypted memory sticks

It is recommended that Corporate documents are stored on the corporate network so that they are held on servers which the Council controls and backs up regularly.

The Council has no control over what happens to data once it leaves the corporate network and cloud services such as Dropbox and SkyDrive are not considered to be secure. Dropbox in particular has been the subject of high-profile data breaches where passwords have been compromised and unauthorised access gained to data held there. The Council rejects requests for access to Dropbox and SkyDrive unless the user can guarantee that the data they will transfer has no sensitivity and can be in the public domain.

Therefore before storing any sensitive data on cloud websites such as Googledrive, Skydrive, Dropbox, etc., you need to ensure you have adequate protection in place to ensure that you do not breach the Data Protection Act.

Schools may store documents on Redstor, which is a secure encrypted cloud service.

The DPA requires that sensitive personal data is not sent outside the European Economic Area (EEA) without ensuring that data is provided with the same or better protection than afforded within the EEA. Therefore the use of some cloud services may breach this principal as many of these services are hosted on servers based outside the EEA. More information can be found at http://www.ico.gov.uk/for_organisations/data_protection/overseas.aspx

Schools and Academies are their own Data Controllers and each school or academy therefore has the same responsibilities under the Data Protection Act to protect the data they handle against unauthorised access. Each school or academy should be aware of where its sensitive data is stored, who has access to it and how it is controlled. A risk based approach taking into consideration data sensitivity should be adopted before deciding whether cloud storage is appropriate or not for your school or academy.

In the United Kingdom the Information Commissioners Office oversees compliance with the Data Protection Act. Schools and Academies should be aware that the ICO has the powers to fine organisations up to £500,000 per data breach. You can view details of organisations that recently have sustained data breaches at http://www.ico.gov.uk/what_we_cover/taking_action/dp_pecr.aspx#undertakings

The ICO has produced guidance on cloud computing which can be found at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/cloud_computing.aspx

Schools’ email travels over the open internet; therefore sensitive and personal information should not be transmitted this way unless it has been properly protected or the school has deemed it an acceptable risk.
Security Advice on Use of Cloud Storage and Transmission of Data

School staff should use their school email address rather than their personal one for anything related to school business. Using a .sch.uk email address will give external recipients more confidence that the email has come from a valid school address. It also presents a professional appearance and keeps all school documentation together.