

Following discussions with suppliers, Becta was asked to obtain assurance from the Information Commissioner's Office (ICO) that the use of the Systems Interoperability Framework (SIF) to share data is legitimate under the Data Protection Act 1998.

Becta and the SIF Association UK welcome the ICO's view that they "... can see no reason why the use of SIF should present any difficulties in respect of compliance with the Data Protection Act 1998."

We also welcome the suggestions and recommendations regarding Fair Processing Notices, penetration testing, training and information governance. These are areas that the SIF Association is aware of and is incorporating in to implementation guidance for organisations who are adopting SIF.

*John Chapman
Penny Murray
Becta*

*e-mail: john.chapman@becta.org.uk
penny.murray@becta.org.uk*

19/2/2009

Dear John,

Thank you for your e-mail enquiry dated 17/2/2009 regarding the legality of the Systems Interoperability Framework (SIF) under the DPA.

I understand from the documents you have forwarded and from our telephone conversation that SIF is a set of interoperability standards which enable information to be shared between a number of applications regardless of the platforms which host them. BECTA believes that increased interoperability will enhance vertical and horizontal reporting and information sharing within the education sector. BECTA also feels that electronic transfer of information will be more secure than other methods. It is also clear from the information I have to hand that SIF is intended to be used to share information which is currently shared by other methods.

Lawfulness

BECTA's concern is whether, or not it will be lawful under the Data Protection Act 1998 to use the SIF system as a framework for sharing information internally between different departments in schools, externally to local authorities, other educational application such as MIAP and the DCSF. The ICO cannot comment on whether the use of SIF will be lawful in terms of the

Act. SIF is a tool, the circumstances of its use and day to day adherence to the DP principles will determine if information shared by SIF has been shared in a manner which complies with the Act. In other words compliance depends on how organisations use their tools, rather than on the tools themselves.

Security

Secure e –systems for transfer of information are well used and understood and it is for BECTA to determine whether the technical safeguards within the SIF framework are adequate for the type of information sharing being done. BECTA should remember that there may be wider concerns than the technical aspects of the SIF. For example, not all information held on school files about children will be sensitive information as defined by the Act, but many members of the public regard all information about children as “sensitive”. In addition there is an atmosphere of decreasing public confidence in government led IT projects so care should be taken to be open with young people and their families about what is happening with SIF. This would also be a good opportunity to make any necessary amendments to privacy notices or fair processing statements.

It might also be useful for BECTA to consider some external and internal penetration testing. Will it be possible to break into the system and follow a trail of interoperability to access or compromise information? Are internal systems secure enough to prevent staff from accessing information which was previously unavailable to them? Does BECTA have technical assistance in place for organisations moving to this system for the first time, or will this be provided by SIF? Is there a general disaster recovery procedure for educational organisations?

Once the SIF system is deployed care must be taken to control access to information. When information is shared across a range of departments there is the possibility that some individuals will have access to a wider range of information than before. Our view is that access to information should always be minimised and an individual should only see what they absolutely must see in order to do their job. This might be a good opportunity to consider access controls in general. For example access could be governed by use of a password or a token or both. In circumstances where the flow of information is being increased it might be useful to consider increasing the security surrounding access. This would also apply in areas where security has previously been a concern or where staff may need to access sensitive personal data.

One of the most important aspects of security is staff training although this is often neglected. When any new technology is installed this presents an opportunity to ensure that all staff have had training in information security and data protection as well as in the use of the new system. This kind of training should be readily available and should be refreshed on a regular basis so that all staff continue to be aware of the importance of their role in keeping information safe. Staff can be either the strongest or the weakest link in any organisation, and the best policies, procedures and equipment cannot insure against the actions of poorly trained staff.

Additional purposes

Fast and efficient information sharing will often generate new ideas about the use of the information available. If an organisation proposes to share information with any other organisation or use it for a new purpose they must ensure that this is necessary, proportionate and transparent. Any new purpose needs to be compatible with the original purpose for which the information was collected.

I have some concerns about the statement in the FAQ document that “clients” in the public sector will pay for SIF mechanisms. I would be grateful if BECTA could clarify this statement. I am assuming that these would be the bodies which intend to use the SIF mechanisms please let me know if this is not the case.

Information governance

The ICO view is that it is vital to have information governance at the heart of information handling. Where large groups of discrete organisations are processing personal information there must be some central control over how this is done. This is beneficial to the organisations themselves as it tends to harmonise policy, guidance and procedure. This simplifies the process of learning new methods of work. A central body can also set out rules relating to data cleansing or security for example. A governance group should also be where security breaches, problems with the system or difficulties with any method of working are reported. This group should set out sanctions for any misuse of personal information whether accidental or deliberate. It should also have monitoring systems in place to ensure that information handling is compliant with the Act.

I note that SIF has a board but it is not clear from the documents I have whether this is intended only to provide governance over development of or access to SIF systems or whether its remit covers information handling in general. I would be grateful if you could clarify this point.

I hope this information will be helpful to you. From the detail I have I can see no reason why the use of SIF should present any difficulties in respect of compliance with the Data Protection Act 1998. However, BECTA should bear in mind that no system is foolproof. The faster more efficient movement of more information across more systems is likely to have some unintended consequences in terms of data protection and use of SIF should be particularly carefully monitored as it rolls out.

If there is anything else you need on this topic, or if you feel that a meeting would be helpful please let me know.

Yours sincerely

*Lynne Shackley
Data Protection Practice Manager – Public Sector*