States of Jersey

Subject:	**Use of Web Based Applications in Schools Policy**
Author:	**Head of Governance, Education Department**
First published	**November 2013**
Last updated	**August 2016**

1. Introduction

In 2012, the Treasury commissioned a data protection audit of the Education Department.

Considered together with a further review commissioned by the Data Protection Commissioner in 2011, these reports have highlighted several notable issues around data protection and information safety within schools and the Education Department in general.

Failure to comply with the Data Protection Law may result in legal action being taken against schools (who are data controllers in their own right). This policy has been developed as there is a pressing need to respond to the issues raised in these audits.

2. Implications

This policy concerns web based applications currently and potentially used by schools and the data protection risks associated with them. Any risk they assume by signing up to web based packages is their responsibility, (not the Department's responsibility) as they are data controllers in their own right. Terms and conditions should be thoroughly read and the potential consequences of signing up to the packages should be seriously considered.

If schools agree to transfer data outside of the European Economic Area (EEA) then they should be are aware they are in breach of their Data Protection terms of notification (registration).

3. Background

A large number of schools have signed up to use web based educational applications, while several others are currently planning to, and have contacted the Department for advice.

While these educational web based packages may have some value, there are some significant risks identified with using them without first undergoing a risk assessment. The terms and conditions attached to some of these sites expose personal pupil data to potential vulnerabilities. There are two broad concerns i.e. legal and safeguarding.

4. Safeguarding Concerns

Schools are acting in loco parentis in agreeing to the sharing of children's personal data by signing terms and conditions on their behalf. In most cases, parents are unaware that the schools are signing up to these packages. If a parent were to look up any school registration on the Information Commissioner's website, it states that their registration does not allow data to be shared outside of the EEA. This could be viewed as providing false assurance. Therefore, the responsibility assumed by schools is significant, as there are risks regarding the eventual destination of children's personal data.

5. Legal Concerns

Schools are all data controllers in their own right. The data protection notification (registration) of all schools in Jersey is limited so that they can only transfer data within the European Economic Area (EEA). However, most of these web based packages do share data outside of the EEA. Both civil and criminal action can result from data protection infringement. Therefore it is important that schools, as data controllers understand the implications of the data protection and contractual arrangements they make when they agree to the terms and conditions of these packages.

6. Schools in the UK

It is worth noting that many schools in the UK also used web based applications that share data outside of the EEA. Therefore, these schools are also rendering themselves liable to prosecution for non-compliance with UK data protection laws. Some schools have bespoke data sharing agreement with companies such as Yahoo which specify that data cannot leave the EEA.

7. Educational Use of web based packages

It is clear that some of these web based packages do have educational value for learning, exam preparation and so on. The Professional Partners are of the view that web based packages, while useful, are by no means essential to education.

With this is mind it may be more appropriate for the onus to be on schools to justify the benefits of the packages rather than 'buying now and thinking later.' The potential benefits of any package should be weighed against the potential risks.

8. Terms and conditions

In brief, in signing up to some packages, schools might be agreeing to the following:

- Children's personal information can be shared with partner companies who operate outside of the European Economic Area (EEA), including countries which are classed as 'inadequate' in data protection terms. *This is in breach of the Data Protection Law. Also, there would be little or no legal redress if a child's data was used inappropriately.*

- This information may also be passed on if any third party company (from any country) 'acquired' the company. *The school has no control over where the data ends up.*

- Children's usernames (which may well be their real name) could be published on the website along with their personal profile, which will include any other personal information that the child has uploaded. That profile will also be indexed by search engines. Obviously the child will not be aware of the implications of this. *A significant picture of a child's name, location, age etc. could potentially be built up by any third party, globally. They would not have to 'hack' the site to do this as the information would be published.*

- It could also be agreed that the terms and conditions can be changed at any time, and it is up to the schools to come back and check the 'small print'.

- If a student or teacher breaches the terms and conditions (e.g. by publishing the website's copyright artwork) then the school could agree to pay all legal expenses arising from any lawsuit.

- This site may link to external websites (likely to be dynamically generated adverts) which could potentially contain unsuitable or insecure content (even the link itself could contain an unsuitable image or words) and the school may, as part of agreeing to the terms and conditions, agree to take complete responsibility for this.

9. Conclusion

When considering signing up to web based packages, schools should carry out a risk assessment and consider carefully any legal and safeguarding implications.

Schools should be fully cognisant of the fact that by agreeing to certain terms and conditions, they would be in breach of the Data Protection (Jersey) Law 2005. They should not sign up to packages which involve personal data leaving the EEA or "adequate" jurisdictions under their current notification.

10. Required Actions

a) Schools should review the web packages that they have already subscribed to, and to unsubscribe if they feel (given the above advice) that those packages are not appropriate. As many packages renew automatically this will require proactive measures.

b) In the future, no web based application should be signed up to without a full risk assessment and consideration of the above. No web based package should be signed up to by any member of staff without the sanction of the head teacher in question.

c) All schools wishing to use web based applications and services should complete the associated training and risk assessment. The school should also nominate an individual within the school to be responsible for the assessment and ongoing monitoring of web based packages, and name this individual on the form. This form should be signed by the Head and designated data protection officer in the school and returned to the Department. In addition, if the school wishes to apply to the Information Commissioner's Office to change their registration to 'worldwide', then this application should be copied to the Head of Governance at the Department.

d) If the software provider is acting as a data processor (as defined by data protection legislation), it is incumbent upon the data controller to put a written agreement place to ensure the security of the data being processed.

N.B. If there is a data protection breach as a consequence of using web based packages, the school and not the Department would be responsible and liable for prosecution as a data controller.