Safeguarding Data – Using Technology: Keeping Pupils Secure in a Connected World

Statement of Purpose

This paper reflects on the growing concerns of schools, education professionals and government about the security of pupil data related to the range of cloud computing tools. It discusses moral and legal issues while signposting examples of advice and good practice.

About the Author

Allison Allen is Director of Outstream Consulting, a Trustee of the Board of Management of Naace and a MirandaNet Fellow; she works with government, business, charities and education organisations. Allison is joint author of several publications including the national e-safety guidance for FE & Skills, the textbook 'Introducing Computing: A Guide for Teachers' (Routledge) and Naace's Curriculum Framework

She taught for many years before joining a large Local Authority as senior ICT Adviser in School Improvement, later becoming a director of the London Grid for Learning and Chair of the pan-London Teaching and Learning action group. Subsequently Allison joined Becta as the London Regional Manager.

With a proven track record at senior level within the education sector, Allison is known to be impartial, objective and independent with keenly developed analytical, presentational and oral and written communication skills.

Contact; allison.allen@outstream.co.uk

Contents

Statement of Purpose 1

About the Author 1

Using technology in a connected world 3

- Head in the Cloud or Sleepwalking? 5
- Examples to consider – has someone in your school agreed contracts like these? 6
- What the law says: 7
  - The eight principles of the Data Protection Act 7
- To decide 'appropriate measures' you need to ask key questions: 8
- If it all goes wrong – what happens? 8
- Advice and good practice 8
- Breaking News – the bigger picture: 9
- Finally 9

Useful Links 9

Endnotes 10

Photograph: Alamy www.alamy.com via The Guardian

Using technology in a connected world

It is fundamental to success that learning can take place in a safe physical or virtual space as described by TED prize-winner, Sugata Mitra;

> *"We need a pedagogy free from fear and focused on the magic of children's innate quest for information and understanding"*

Figure 1 Sugata Mitra's 'Hole in the Wall' experiment[i], leading to SOLE[vi] thinking

What do we mean by education in a connected world? The School in the Cloud[ii] is a new idea from Sugata Mitra, based on concepts such as that of personal learning networks (PLN) which are themselves related to the theory of connectivism developed by George Siemens and Stephen Downes[iii] where learners create connections and develop a network that contributes to their development and knowledge. Learners tend to develop informal personal learning networks[iv] (PLNs) that are made up of the people with whom they interact and from whom they gain knowledge, as well as the technologies that support such communication and knowledge exchange. Flipped learning[v] extends these ideas so that knowledge gathering and research is done outside the classroom, leaving lessons available for developing thinking and debate. In many schools cloud technologies are used to support collaboration in flipped learning.

Feeling safe is a basic and fundamentally important need. It is well known that when learners (children and adults) do not feel safe, it undermines learning, teaching and healthy development.

New teaching and learning pedagogies such as SOLE[vi], PLNs (Personal Learning Networks) and Flipped Learning depend on the learner feeling safe - all require teachers to not only consider e-safety issues in the classroom, but to address issues of safeguarding. School and college staff have a responsibility to provide a safe environment in which children can learn; the term 'e-safeguarding' addresses all safeguarding issues which relate to the use of ICT and includes e-security and e-safety. Senior managers also need to think about the whole school culture as virtual spaces, storage and tools become part of the learning landscape.

E-security is not just about children; in 2014 there was a widespread concern that patients' NHS data (similarly HMRC) had been collected by authorised consultants who then passed it to Google analytics; although anonymised, it was possible to identify individuals and we do not know who the Google operatives were or where they were in the world. Similar activity has been uncovered in April 2015.

The concern about data isn't confined to the UK; in America (2014), Secretary of Education Arne Duncan reaffirmed that school systems "owe families the highest standard of security and privacy." He continued "What I want to say to you today is that the benefits for students of technological advancement can't be a trade-off with the security and privacy of our children. We must provide our schools, teachers and students cutting-edge learning tools. And we must protect our children's privacy. We can and must accomplish both goals – but we will have to get smarter to do it."

In most schools the Head Teacher/SMT is the Senior Information Risk Officer (SIRO) and Data Protection Officer - sometimes the two are combined but in some schools teachers are not aware of who that person is. If we handle and store information about **identifiable, living people** – for example, about school pupils – we are **legally obliged** to protect that information. The Data Protection Act states that we must only collect information that we need for a specific (specified) purpose and keep it **secure**. Many schools follow good practice, but not all.

With increasing availability of these tools matched by constraints on school budgets, tensions are emerging. We were shocked that an educator expressed doubt that any school in the country really feels this law applies to them! In our experience schools are totally concerned to protect their pupils and take their obligations under the Data Protection Act - one of our most powerful laws, very seriously.

Password protection is only a fraction of the answer – even second factor enabled is not enough!

The Naace ICT Mark[vii] is the national benchmark for schools' good use of technology and recognises good practice in all areas of the use of technology across the school curriculum and management. ICT Mark schools are at the forefront of good, creative and purposeful use of technologies to support teaching, learning and school administration. Schools use this award to drive change and many are, or go on to be, outstanding. A question that ICT Mark Assessors are increasingly asked is related to the use of 'free' technologies such as **cloud storage and productivity tools**, and the security of pupil and staff data.

Recently we were astonished during a supplier presentation to hear that schools allowed them to use identifiable pupil data for demonstration; the presenter went on to show the platform product full of the names, addresses, ages and details of current school pupils. He saw nothing wrong.

Head in the Cloud or Sleepwalking?

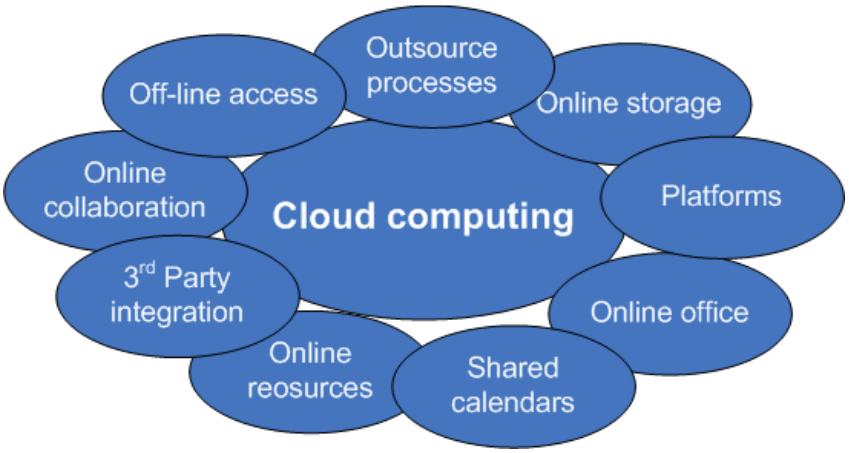

Figure 2 Cloud opportunities (pubs.sciepub.com)

It is easy to identify the benefits of using cloud computing in school, especially when the product has little or no monetary cost compared to being tied in to a Local Authority offering which often include substantial (if undervalued) support for security and training. It is also very easy to tick the box that means you agree with the terms and conditions of use – although many busy people at best skim-read 56-page, densely written documents. If we keep our finances secure, how much more important is keeping personal information about our pupils safe?

Without sufficient security measures and collection regulations, cloud computing could put sensitive pupil information at risk for unwanted marketing uses and public disclosure, and may put children at a higher risk of fraud – did you know that children's' identities are highly desirable to fraudsters as they are 'clean and fresh' and have no County Court Judgements (CCJs)?

Researchers at Fordham Law School found that a majority of the service partnerships between cloud service companies and schools lack sufficient oversight, specifically regarding what happens to data *after* a third-party company receives it. Less than 25 percent of the contracts studied, specified the purposes for sharing student information and less than 7 percent restricted the sale or marketing of shared information by vendors. Many agreements allow vendors to change the terms without notice. "People know if they hack into them they can get several schools' information instead of what they would get if they just went after a single institution."

The results (unpublished) of short survey of schools conducted by the ICO at the end of 2014 showed over 50% of school respondents did not know the answers to some key questions about the secure use of cloud services and their responsibilities under the DPA. They did not understand or had not read the terms, conditions and privacy policies that formed the school's contract with the cloud supplier. Children are already at a high risk of becoming victims of identity theft. It is worth getting your school Bursar, Finance Officer or SIRO to look at the agreements.

Examples to consider – has someone in your school agreed contracts like these?

- This extract is from a new free learning platform built for schools, free to use, the popularity of sign-ups is increasing and it is hosted on Amazon servers (supplier identifiers are redacted):

  "If you submit #content# you grant '#######' a non-exclusive, worldwide, perpetual, irrevocable, royalty-free license to use, modify, adapt, publish, translate, perform, make searchable, convert into another format, and create derivative works from and/or distribute your #content# for any purpose. Additionally, by posting/uploading #content#, you further grant all users of the service and anyone who obtains the #content# via an external search engine, a non-exclusive, worldwide, perpetual, irrevocable, royalty-free license to use, modify, adapt, publish, translate, perform, and create derivative works from and/or distribute your #content# for any purpose." (Note: Content may be information about pupils and/or staff).

- Below is our analysis of the Terms and Conditions of an anonymised supplier of Cloud storage to schools including Multi-academy trusts (MATs) and Diocese clusters.

  - The T&Cs are written in legally dense 'lawyer' terms – hard for schools to understand and appear more appropriate to business
  - Possible immediate loss of access to data
  - No notice changes to products
  - Automatic deletion of stored data on expiry etc of subscription (schools must keep data for 7-10 years after the pupil has left)
  - Schools have to find alternative backup
  - Third party product without warranty (allows third party access)
  - Disclaimed warranty for fitness for purpose, security, quality etc
  - No warranty that third party/beta version (current) will be error free or that security will be secure or effective
  - Risk via unencrypted transmission via internet

- Do very careful checking of the Terms and Conditions and Privacy Agreement on Google Apps for Education, Amazon, Drop Box and so on. This is extracted from Google Docs T&Cs:

  "When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content..... This license continues even if you stop using our Services".

Make sure too, that you know where in the world the information (data) is stored, who has access and if the location complies with our Data Protection laws. It is surprising how much stronger our law frequently is!

- From Google Apps for Education (aka GAFE)

  1.1 Facilities and Data Transfer. ... As part of providing the Services, Google may transfer, store and process Customer Data in the United States *or any other country in which Google or its agents maintain facilities.* By using the Services, *Customer consents to this transfer, processing and storage of Customer Data.*

  And critical in the context of pupil data; ....."*Google is* merely *a data-processor*"

  FERPA[viii] and COPPA[ix] do not apply to the UK and our pupils thus have less legal protection when using cloud hosted outside the EEA

  ..."Customer acknowledges and agrees that it is solely responsible for compliance with the Children's Online Privacy Protection Act of 1998, including, but not limited to, obtaining parental consent concerning collection of students' personal information used in connection with the provisioning and use of the Services by the Customer and End Users."

  "After termination *customer data is deleted*/terminated" - In order to comply with the Data Protection Act and the needs of its community, a school need secure backup of information about pupils, staff and governors – and that requirement lasts for 7-10 years after they have left the institution. It is therefore ironic that cloud storage is unsuitable to store such data unless it is backed up securely elsewhere.

What the law says:

The Data Protection Act 1998 (DPA1998) regulates the processing of personal data relating to living individuals (data subjects e.g. pupils/staff), imposes legal obligations upon data controllers (e.g. schools/governors), provides data subjects with legal rights in respect of the way their personal data is processed, introduces criminal and civil sanctions for breaches and is enforced by the Information Commissioner's Office (ICO). The ICO is a really useful source of help and advice.

Data controllers are obliged to register with the Information Commissioner's Office – most schools register at least twice (pupils and staff data). Schools have to state the purpose(s) for which data is stored, list to whom they will disclose data (this includes organisations like the LA, FE colleges, Ofsted) and for how long it is stored – generally pupil and staff data is stored for about 7 years – this relates to exam results requests or references and financial data for 6 years.

The eight principles of the Data Protection Act

1. Fair and lawful processing
2. Processed for limited & specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than necessary
6. Processed in line with individuals' rights

7. Kept appropriately secure*

8. Not transferred outside the EEA without adequate protection

*"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

To decide 'appropriate measures' you need to ask key questions:

- ☑ *What's the risk?*
- ☑ *What do we do with personal data?*
- ☑ *Collection, storing, using, disposal - how valuable, sensitive or confidential is the data?*
- ☑ *What damage or distress could be caused to individuals if there was a security breach?*
- ☑ *How can we minimise the risk?*

There is a useful presentation here that will help you consider various scenarios: http://ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/ico_presentation_20140508-ISBA-annual-conference-Victoria-Cetinkaya.pdf

If your website/Learning Platform/Cloud Computing/storage includes personal information about pupils or teachers, Principles 7 and 8 are likely to be engaged - Principle 8: Personal data not transferred outside the EEA without adequate protection.

- ☑ *Is it hosted outside the EEA…..?*
- ☑ *Not sure…..?*

If it all goes wrong – what happens?

Complaints to school and to the ICO, enforcement notice, increased level of audit, criminal prosecution and monetary penalty – the last can be severe and largely relates to Principles 7, plus 4 and 5. For example, loss or theft of unencrypted devices (highest penalty £150,000 to date) or insecure disposal, both paper and electronic (highest penalty £325,000 to date) and insecure websites/online networks (highest penalty £500,000 to date)

Advice and good practice

There are some safeguards to help as well as links at the end of this paper. Most schools are connected on the NEN (National Education Network that runs on SuperJanet, usually via the Regional Broadband Consortium (RBC). Janet negotiated changes to Google's standard Apps for Education Agreement (as they did for Microsoft O365) and that this is the basis of the JISC advice and Framework which gives schools some security. http://www.jisc.ac.uk/news/jisc-signs-framework-agreement-with-google-apps-for-education-08-oct-2013

More information is available at HTTPS://www.ja.net/product-services/Janet-cloud-services/Google-apps-education

Some RBCs have developed additional services hosted on the UK NEN such as online productivity tools like LGfL's MyDrive and SWGfL's 'Cloud PC' cloud storage

Breaking News – the bigger picture:

"The European commissioner who could soon be co-leading the EU's digital agenda has wasted no time in firing warning shots at the US over data protection.

Andrus Ansip used his confirmation hearing before the European Parliament yesterday to warn that the EU might suspend the Safe Harbor[x] data-sharing agreement if US lawmakers don't get their act together when it comes to protecting European citizen's data. "Safe Harbor is not safe to today," the 58-year-old former Estonian prime minister said. "Americans have to provide real trust to European citizens. When it comes to protecting data, similar rules and safeguards should apply to all companies wherever they are based. To be worthy of their name, Safe Harbors do need to be safe.

Suspending the data agreement would have major implications for companies such as Google, Facebook and Microsoft, among others, that process data in the US from European citizens. EU laws prohibit the transfer of personal data to non-EU countries that do not meet the EU's data-protection standards. As part of Safe Harbor, US companies are supposed to meet EU standards in providing data protections for Europeans.

But European citizens are really worried about how the US uses its national security exception, Ansip said. "If we will not get clear answers on how this exception will be used, then of course suspension as an option will stay on the table," he said." (Loek Essers|IDG News Service)

Finally

According to a research team from UC Berkeley[xi] [Armbrust, Fox, et al, 2009], cloud computing embodies the long-held dream of computing as a utility and has the potential to transform, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. It offers elasticity of resources without paying a premium, and refers to both the applications delivered as services over the Internet - Software as a Service (SaaS) and the hardware and systems software in the data centres that provide those services – what we call a Cloud.

We do not suggest schools avoid the benefits Cloud can offer, but we do advise them to consider any potential risk to their school community. This does mean identifying and following good practice regarding all the legislative, ethical and moral issues regarding the safekeeping of pupil data. There are many examples of compliant suppliers – the usefully short, plain English T&Cs from 2Simple for example, explain conformity with the DPA and their use of UK servers while Groupcall have a similar enlightened approach.

Useful Links

Ken Corish's excellent blog on this topic http://66.147.244.88/~kencoris/standing-out-from-the-cloud/

SWGfL Policy Guidance http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy/Content/School-Personal-Data-Handling-Policy.aspx

LGfL Data Security Advice http://www.lgfl.net/esafety/Pages/data-security.aspx

ICO overview presentation - Love new technology: hate data protection compliance? http://ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/ico_presentation_20140508-ISBA-annual-conference-Victoria-Cetinkaya.pdf

ICO Data Responsibilities and Cloud Storage http://ico.org.uk/news/latest_news/2012/cloud-on-the-horizon-for-data-handling-outsourcing-27092012

ICO Report on schools' data protection guidance 2012: http://www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx

ICO guidance – www.ico.org.uk

Discussion - Are schools putting your child's information at risk? http://www.creditcards.com/credit-card-news/schools-student-personal_data_privacy-cloud-1282.php

NEN Cloud advice - http://www.nen.gov.uk/cloud-computing/

DfE advice on data protection for schools considering cloud software services for local authorities, school leaders, school staff, governing bodies and applicable to all local authority-maintained schools, academies and free schools. It includes suppliers' self-certification checklists. https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Student information in the US and EU https://refeds.org/docs/FERPA-DPD%20v1-00.pdf

Endnotes

[i] After a series of experiments revealed that groups of children can learn almost anything by themselves, researcher Sugata Mitra began his pursuit to inspire children all over the world to get curious and work together. In 1999, Sugata and his colleagues dug a *hole in a wall* bordering a slum in New Delhi, installed an Internet-connected PC, and left it there (with a hidden camera). Soon, they saw children from the slum playing with the computer, learning English and searching through a wide variety of websites on science and other topics, and then teaching each other.

[ii] https://www.theschoolinthecloud.org/

[iii] Siemens, G. (2005) Connectivism: A Learning Theory for the Digital Age, *International Journal of Instructional Technology and Distance Learning*, Vol. 2 No. 1, Jan 2005

[iv] https://en.wikipedia.org/wiki/Personal_Learning_Networks

[v] http://flippedlearning.org/

[vi] http://www.ted.com/prize/sole_toolkit

[vii] The ICT Mark is a nationally recognised quality accreditation that schools can achieve once they reach a certain level of maturity and have completed the commentary sections in the online Self-review Framework tool. The accreditation celebrates the considerable achievement of schools that have developed their use of technology to support learning to represent solid good practice. http://en.wikipedia.org/wiki/Self-review_framework

[viii] The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. It does not apply to institutions that do not receive funding under Department of Education programmes

[ix] The Children's Online Privacy Protection Act of 1998 (COPPA) is a United States federal law. It applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It includes details of a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. While children under 13 can legally give out personal information with their parents' permission, many websites disallow underage children from using their services altogether due to the amount of cash and work involved in the law compliance. It does not prevent children from lying about their age

[x] The decision by U.S. organisations to join the Safe Harbor program is entirely voluntary and relies on annual self-certification.

[xi] http://ftp.cs.duke.edu/courses/cps296.4/compsci590.4/fall13/838-CloudPapers/AboveTheClouds.pdf