JISC cetis

centre for educational technology
& interoperability standards

Analytics Series

Vol.1 No6.: Legal, Risk and Ethical Aspects of Analytics in Higher Education

By David Kay (Sero Consulting), Naomi Korn and Professor Charles Oppenheim

CETIS Analytics Series ISSN 2051-9214

Produced by CETIS for JISC

Legal, Risk and Ethical Aspects of Analytics in Higher Education

David Kay (Sero Consulting Ltd) with input from Naomi Korn Consultancy & Professor Charles Oppenheim

Table of Contents

1. Executive Summary

1.1 SCOPE

The collection, processing and retention of data for analytical purposes has become commonplace in modern business, and consequently the associated legal considerations and ethical implications have also grown in importance. Who really owns this information? Who is ultimately responsible for maintaining it? What are the privacy issues and obligations? What practices pose ethical challenges?

This paper in the CETIS Analytics series covers legal, ethical and related management issues surrounding analytics in the context of teaching, learning and research and their underlying business processes. It is based on current UK law, set in the context of publicly funded Further and Higher Education and their mission. With a primary focus on personal data, it considers the rights and expectations of the data subjects (students, researchers, employees) and the responsibilities of institutions, above campus services, suppliers and funders.

1.2 CORPORATE CONSIDERATIONS

The types of personal data under consideration may have been collected for some years in a variety of IT systems, yet largely not utilised for analytical purposes. However, there are now compelling motivations driving the development of analytics capabilities in the sector:

- Responses to economic and competitive pressures may be derived from business intelligence.
- Analytics practice is strongly linked to modern enterprise management.
- Users, especially born digital generations, appear increasingly to expect personalised services that are responsive to profile, need and interest and are therefore more likely to be content for their data to be used to those ends.

In considering the collection and processing of such data, institutions need to balance risks and rewards with legal and policy obligations as well as with the expectations of their community:

- Aligning use of personal activity data and business intelligence with their overall mission and motives.
- Weighing the benefits and costs of putting in place policies, procedures and tools for organisational legal and risk compliance.
- Adapting governance frameworks and developing staff awareness to cover the responsibilities relating to such data.
- Taking account of capture and exploitation of student or researcher activity data outside direct corporate controls by individual academics and service providers including shared services.

However, exercise of due diligence is hampered by the speed of developments in the online world and the pressure not to be left behind as institutions compete for students and for research funding.

- The level of legal 'maturity'; There is a lack of precedent to indicate the application of the law in the digital environment and therefore there remains uncertainty about legal interpretation.
- Comparable ethical settings; Bearing in mind therefore that practice and precedent in education is relatively under-developed, useful exemplars might be found in research and medical ethics and in retail and online consumer services; however, there remains an underlying question as to whether education is in some respects special.

1.3 THE DATA AND THE LAW

The factors described above can serve to generate a degree of fear, uncertainly and doubt, even given the opportunity to apply legal assessments and ethical principles backed confidently elsewhere in society. It is in the light of such expectations that this paper explores legal considerations, highlighting issues and mitigations that will enable institutions to progress their use of analytics whilst managing risk to the benefit of the individual, the institution and the wider mission of education.

The legal and ethical considerations relating to analytics are focused on personal data processed by or on behalf of the institution. Whilst other corporate data, in areas such as financials or estates, present their own technical, operational and interpretative challenges, they do not raise such immediate legal and ethical issues relating to individuals. Such personal data of analytical value may range from formal transactions to involuntary data exhaust (such as building access, system logins, keystrokes and click streams). The data can be derived from a range of systems:

- Recorded activity; student records, attendance, assignments, researcher information (CRIS).
- Systems interactions; VLE, library / repository search, card transactions.
- Feedback mechanisms; surveys, customer care.
- External systems that offer reliable identification such as sector and shared services and social networks.

Under UK law, the practice of analytics, especially with reference to personal data, should be considered under the headings of Data Protection, Confidentiality & Consent, Freedom of Information, Intellectual Property Rights and Licensing for Reuse.

In the light of the legislation and the guidance of the Information Commissioner, and subject to adoption of good data governance, training and active risk management, this paper reflects on low levels of risk and proposes responsible mitigation in keeping with the reputation, mission and business imperatives of the sector.

1.4 ETHICAL DIMENSIONS

Given the education mission and associated governance responsibilities, broad ethical considerations are crucial regardless of legal obligation. This impacts broad considerations and concerns about the use of personal data, as well as the specific uses involved in analytics.

- Variety of data - principles for collection, retention and exploitation.
- Education mission - underlying issues of learning management, including social and performance engineering.
- Motivation for development of analytics – mutuality, a combination of corporate, individual and general good.
- Customer expectation – effective business practice, social data expectations, cultural considerations of a global customer base.
- Obligation to act – duty of care arising from knowledge and the consequent challenges of student and employee performance management.

We compare these considerations with the experience and resulting norms in the research, consumer and social network domains. Research ethics provide a valuable basis for thinking about the issues raised by analytics, with the added advantage of recognition within the educational community. The practice adopted by leading business to consumer players provides a clear and legally grounded approach that is likely to be readily understood by the public in much of the world.

More radically, some commentators emphasise the imperative to review and even to revise ethical considerations on account of the increasingly widespread adoption of online transaction with its associated activity-based and social feedback loops. In this ‘brave new world’ there is a will, even a presumption of necessity, to trade privacy for other benefits within the new social economy. However, others such as Keen (‘Digital Vertigo’) and Lanier (‘You are not a Gadget’), have pointed to the personal and societal downsides of an online data-driven culture.

Furthermore there is danger in assuming that ethical considerations are universal and therefore promoting the transferability of norms across cultural and domain boundaries – in this case adopting norms established about the use of personal data for analytical purposes in domains such as research, consumer services and social networks.

So the challenge is whether the education community, not least in the emerging field of learning analytics, should revise its ethical position on account of the changing attitudes and expectations in the digital realm with which learners and researchers are increasingly associated. At the very least, even if ethical norms are not immutable or self-evident, practice in other sectors suggests candidate approaches.

1.5 GUIDING PRINCIPLES

As Voltaire's Candide might have reflected, we are faced with the imperative to seek out the 'best of all possible worlds':

- **In assuring educational benefits**, not least supporting student progression, maximising employment prospects and enabling personalised learning, it is incumbent on institutions to adopt key principles from research ethics.
- **As businesses**, post-compulsory educational institutions are facing the same business drivers and globalised competitive pressures as any organisation in the consumer world.
- **To satisfy expectations** of the 'born digital' / 'born social' generations, there is a likely requirement to take on ethical considerations, which may run contrary to the sensibilities of previous generations, especially in respect of the trade-off between privacy and service.

Notwithstanding these tensions, we conclude that there are common principles that provide for good practice:

- **Clarity**, open definition of purpose, scope and boundaries, even if that is broad and in some respects open-ended.
- **Comfort and care**, consideration for both the interests and the feelings of the data subject and vigilance regarding exceptional cases.
- **Choice and consent**, informed individual opportunity to opt-out or opt-in.
- **Consequence and complaint**, recognition that there may be unforeseen consequences and therefore providing mechanisms for redress.

2. Context

2.1 THIS REPORT

This paper in the CETIS Analytics Series covers legal, ethical and related management issues surrounding the generation, use and sharing of analytics data in the context of teaching, learning and research and the underlying business processes.

The report is;

- Based on current UK law.
- Set in the context of publicly funded Further and Higher Education and its mission.
- Focused on the collection, control and processing of personal data, which is a strong focus of the law and which raises particular ethical considerations, both general and educational.

The report takes account of the implications for the wide range of 'actors' involved:

- Rights and expectations of the data subjects – students and their parents / carers, researchers, employees.
- Responsibilities of the supply side - institutions, above campus services, their employees and their functions (for example, teaching, research, registry, finance, quality, marketing, planning, estates).
- Implications for unions, professional associations, vendors / suppliers and funders.

2.2 HIGHER EDUCATION INTEREST

The types of personal data under consideration may have been collected for some years by many institutions in a variety of IT systems, ranging from registry to access control. Typically, such data has not however been used for analytical purposes and may largely have been un-utilised.

However, there are currently compelling motivations to look at the development of analytics capabilities in the sector:

- Responses to economic and competitive pressures may be derived from business intelligence, analytics drawing on a wide range of data available within and beyond the institution.
- Agility of analysis is essential, as the cascade of questions that might be asked within the institution and by third parties is not predictable.
- Use of analytics is expected as good practice in modern enterprise management.
- Sector customers, especially born digital generations, may also expect that good businesses will deliver intelligent personalised services that are responsive to profile, need and interest and are therefore content for their data to be used to those ends.
- Accessible and affordable IT tools now exist not only to organise and to store this large scale data but also to visualize the patterns and trends it contains.
- The unpredictability of questions to be answered by the data implies that it may be counter-productive to perform aggregations motivated by current understanding of the analytical narrative. Aggregations almost certainly impose downstream analytical limitations (for example aggregation typically loses the time precision and may also loose other contextual identifiers). However, storage of raw data raises both legal and ethical concerns.

2.3 LEGAL AND ETHICAL CONTEXT

In considering the collection and processing of such data, institutions will need to balance the risks and rewards of using this data, with legal and policy obligations.[1]

However, such a process of due diligence is hampered by the speed of developments in the online world and the pressure not to be left behind as institutions compete for students and for research funding.

- **Level of legal 'maturity'**; there is a lack of precedent and therefore of case law to indicate the application of the law in the current digital environment; the law (for example, the Data Protection Act 1998) was not specifically designed to accommodate emerging practice in social media, online retail and comparison services and therefore there remains uncertainty about interpretation in the absence of case law.

- **Comparable ethical settings**; bearing in mind therefore that practice and precedent in education is relatively under-developed, it may be useful to look for lessons in other comparable sectors with well-articulated positions regarding consent and customer care. Useful exemplars might be found in research and medical ethics and in retail and online consumer services.

- **Education is different**; there remains an underlying question as to whether education is in some respects special; regardless of legality, it might be suggested that education is, from the perspective of its own practitioners, ethically more sensitive than other sectors.

These factors can serve to generate a degree of fear, uncertainly and doubt, even given the opportunity to apply legal assessments and ethical principles backed confidently elsewhere in society. Indeed, it might be argued that educational legal counsel and established academics provide a mutual reinforcement that is least likely to depart from custom and established practice. However, the new economics of education, the expectations of born digital students and new pedagogies (e.g. geared to personalisation and Massively Open Online Courses [1]) may represent an undeniable tipping point.

It is in the light of such expectations that this paper explores legal and ethical considerations, highlighting issues and mitigations that will enable Further and Higher Education institutions to progress their use of analytics whilst managing risk to the benefit of the individual, the institution and the wider mission of education.

[1] The investigation undertaken by the University of Edinburgh usefully addresses these considerations - http://edina.ac.uk/projects/Using_OpenURL_Activity_Data_Initial_Investigation_2011.pdf

3. Use Cases

The legal and ethical considerations relating to analytics are focused on personal data processed by, or on behalf of, the institution. Whilst other corporate data, in areas such as financials or estates, present their own technical, operational and interpretative challenges, they do not raise such immediate legal and ethical issues relating to individuals.

This section seeks to exemplify the types of data and the modes of collection and of processing that relate to personal data.

3.1 DATA SOURCES

Personal data of analytical value may range from formal transactions (such as assignment submissions) to involuntary data exhaust (such as building access, system logins, keystrokes and click streams).

The data can be derived from a range of institutional systems sources; for example:

- Recorded activity - student records, lecture attendance, assignment submission, research publication, researcher information (CRIS).
- Systems Interactions - VLE, library / repository search.
- Card-based transactions - student / staff card, library card.
- Feedback mechanisms - surveys, customer care.
- General access - to anything digitally controlled through IT systems, such as buildings.

The same individuals could be tracked in any external systems that offer some form of reliable identification such as:

- Above campus shared and sector services ;e.g. Copac, Jorum, HESA, SCONUL Access, UCAS.
- Social networks; e.g. Facebook, Foursquare, LinkedIn, Twitter.

3.2 SERVICE SCENARIOS

Regardless of the type of data or the source application, there is a common range of Use Cases that characterise the service scenarios in which the collection and subsequent control and utilisation of the data take place, as presented below.

For each of these cases, and for any other variants, it is important to understand the following responsibilities, so that issues raised can be considered and where necessary, suitably mitigated:

- Legally - under the law (generally, not just for the purposes of the Data Protection Act), who is the data collector?
- Ethically – regardless of the defensible legal position, what responsibility does the institution or sector service have? This is especially important in the case of above campus and outsourced services.

Whilst our six use cases will often be combined in the flow of analytics activity, it is useful to consider the key legal issues for each individually:

	Use Case	Examples	Main Legal Issues – see Sections 4.1-5
UC1	Institution processing raw data collected upstream.	Use of the university hash tag on Twitter.	4.1 Data Protection 4.2 Confidentiality and Consent 4.3 FoI 4.4 IPR
UC2	Institution using data collected and processed upstream.	Data supplied by UCAS – which may or may not have been anonymised and / or aggregated.	4.1 Data Protection 4.2 Confidentiality and Consent 4.3 FoI 4.4 IPR
UC3	Institution as Collector using data collected from internal systems.	Data used for institutional purposes, such as library resource management or help desk staffing, course re-design.	4.1 Data Protection 4.2 Confidentiality and Consent 4.3 FoI
		Data used for personal purposes, such as learning support, personalisation, advice and guidance.	
UC4	Institution as Collector supplying its data to its subject for personal use.	Data supplied in a transfer format or through an API; there are no known current examples but it is a likely future use case that falls within a logical view of the data subject's rights, especially in a lifelong learning context.	4.1 Data Protection 4.2 Confidentiality and Consent 4.5 Licensing
UC5	The Collector sharing its data with other parties – notably with partners, vendors or customers.	Collection as a franchise operator supplying data to the franchise 'licensor'.	4.1 Data Protection 4.2 Confidentiality and Consent 4.3 FoI 4.5 Licensing
		A publisher as collector sharing usage data with client institutions.	4.1 Data Protection 4.2 Confidentiality and Consent 4.3 FoI 4.4 IPR 4.5 Licensing
		An institution sharing data with regulators or funders; e.g. HESA, REF.	4.1 Data Protection 4.2 Confidentiality and Consent

UC6	Institution as Collector releasing its data publicly as Open Data.	EDINA releasing OpenURL Resolver data.	4.1 Data Protection 4.2 Confidentiality and Consent 4.4 IPR 4.5 Licensing

4. Legal Considerations

Legal considerations associated with activity data (and the associated ethical and risk considerations) can be categorized under the following headings:

- Data Protection
- Confidentiality and Consent
- Freedom of Information
- Intellectual Property Rights
- Licensing for Reuse

4.1 DATA PROTECTION ACT (DPA)

Compliance with the Data Protection Act (“DPA”) is a requirement for organisations involved in processing personal information including information associated with identifiable living individuals. Activity data may be classed as personal information if it can be associated with an identifiable individual.

What makes a difference under the law?

Does the information relate to an identifiable, living, individual?

Data Protection law only applies to information relating to an identifiable living individual. Activity data will therefore escape the DPA’s provisions if it is collected anonymously. The Information Commissioner has recently produced a draft anonymisation code of practice (available at http://www.ico.gov.uk/news/latest_news/2012/ico-consults-on-new-anonymisation-code-of-practice-31052012.aspx). So, for example, where activity data relates to an IP address, unless there is a record of the individual user allocated that particular IP address at that time, the use of the data will not be subject to the DPA.

Who is the data controller?

The law makes the ‘data controller’ primarily responsible for compliance with the Act. The data controller is the person or organisation that lays down the purposes for which the data is going to be used. This may or may not be the same person as the one that collects the data. Anyone who processes the data (including collecting it, calculating or amending it, or transferring it to someone else) is a “data processor” in law. The data controller must ensure that the data processors chosen to process the personal data abides by their DPA duties and obligations.

What must the data controller ensure?

The data controller must ensure that use of the personal data is fair and lawful. That means that the 'data subject' (the person about whom the data relates) must be informed as to the purpose of collecting the data, and that processing of the data must be done under one of the justifications listed in Schedule 2 of the Act (usually that consent has been given, that the data is required to fulfil a contractual obligation to the data subject, or that processing is in the legitimate interests of the data controller). In addition, there must be compliance with the other 'principles' listed in Schedule 1 – that the data is only used for the purpose notified, that where necessary it is kept up-to-date and accurate, and that it is dealt with using security measures (technical and organisational) appropriate to the sensitivity of the data. Other obligations are that the data shall be accurate, and that the data controller must respond to any requests by the data subject to inspect the data held about them.

What happens if the data is anonymised or aggregated?

As long as a living individual cannot be identified from the remaining data, it ceases to be personal data, and the provisions of the DPA no longer apply. However, it is essential to bear in mind that anonymisation and even aggregation does not necessarily prevent identification, notably in cases where the unit of aggregation involves small numbers of data items – for example, courses with small numbers or resources that are rarely borrowed, or residences with few occupants. This matters because the apparently anonymised data may implicitly or indirectly point to a single individual – for example, borrowers of a large print version of a text on a small Masters course.

Would a complaint about personal identification in aggregated data be upheld in law?

If the individual can be identified from this data and the act cannot be justifiably carried out under one of the justifications listed in Schedule 2 of the Act then this might be a potential breach of the DPA. In addition, there must be compliance with the other 'principles' listed in Schedule 1 – that the data is only used for the purpose notified, that it is kept up-to-date and accurate, and that it is dealt with under security measures (technical and organisational) appropriate to the sensitivity of the data. There is no legal objection as such to personal data being processed – the DPA is not a privacy law. The DPA simply provides the framework for circumstances when personal data can be lawfully processed. Therefore, as long as the DPA rules are followed, an individual has no grounds for complaint that their identity can be deduced within a mass of aggregated data. Of course, if it turns out that the personal data breaches some aspect of the DPA, then the individual has grounds for complaint.

What about forthcoming European rules?

In January 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules "to strengthen online privacy rights and boost Europe's digital economy", recognising that "technological progress and globalisation have profoundly changed the way our data is collected, accessed and used." The proposed reforms cover a broad set of emerging data protection challenges, not least raised by social networks, including the "right to be forgotten" (i.e. notwithstanding obligations under the law, to have attributable personal data taken down), and data portability. We should however bear in mind that this is only at a formative stage at EU level, facing the challenge of addressing the widely varied interpretation of the current 1995 rules across the 27 member states, and then the downstream hurdle of incorporation into UK law, so it is not a current consideration or risk.

Further reading about this topic can be found here:

Data Protection Guidance produced by the Information Commissioner's Office
http://www.ico.gov.uk/for_organisations/data_protection.aspx

JISC Legal Personal Data and Consent Management Paper
http://www.jisclegal.ac.uk/Projects/ConsentManagement.aspx

4.2 CONFIDENTIALITY AND CONSENT MANAGEMENT

In UK law there exists a 'duty of confidentiality'. Because it was developed through case law, it is difficult to make clear-cut interpretations.

In some circumstances, the law relating to contracts may apply, and researchers should be aware of this. If an explicit statement of agreement has been made on the extent of the confidentiality to be afforded to the provider of the information (e.g., in a consent form), this may constitute a contract. Disclosure of information subject to such a confidentiality agreement would constitute a breach of confidentiality and possibly a breach of contract. A duty of confidentiality can also arise without an explicit statement of this kind. It may be established in situations where information is sensitive, for example medical details, and when it has been supplied in circumstances in which the recipient might reasonably suppose it to be confidential.

Further reading about this topic can be found here:

JISC Legal Personal Data and Consent Management Paper

http://www.jisclegal.ac.uk/Projects/ConsentManagement.aspx

4.3 FREEDOM OF INFORMATION (FOI)

Universities and colleges need to prepare themselves for external requests for their activity data and information about their activity data in accordance with their responsibilities as outlined within the Freedom of Information Act.

What are the implications in practice?

Could a justifiable request be made for the supply of activity and other like data collected for analytical purposes?

Under Freedom of Information legislation, any third party is entitled to make such a request. The response must be made in such a manner that no personal data is disclosed.

Bearing in mind the potential scale of such data, would an FoI request need to be specific regarding period and category?

No, it does not have to be. There are circumstances where the recipient of an FoI request can refuse to answer a request if it considers the request to be unreasonably broad or deliberately vexatious, but the requestor is then entitled to complain to the Information Commissioner's office about the refusal, and the Institution would have to justify its refusal to the ICO. However, it is common for recipients of FoI requests to encourage requestors to be as specific as possible in their information needs.

Bearing in mind the opaque nature of this type of highly codified data, would an FoI response require a reporting format that indicated the meaning of the data?

Yes, always. The information supplied must be in a form that the recipient can understand it. This can be achieved, for example, by an accompanying document explaining the codes used, or an invitation to the requestor to come in and discuss the contents with someone who can explain their significance.

Further reading about this topic can be found here:

JISC Legal Information on FoI

http://www.jisclegal.ac.uk/LegalAreas/FreedomofInformation.aspx

4.4 INTELLECTUAL PROPERTY RIGHTS (IPR)

Although raw activity data is unlikely to attract copyright, a type of IPR, collations of such data may attract database rights, another type of IPR, which can restrict uses of substantial amounts of this data; enhanced activity data may itself be in copyright and may well enjoy database rights as well. In this case, it is important to understand:

- If there is any IPR, and if so, what type(s)?
- Who might own it?
- If any part of the data is owned by a third party under what terms can it be accessed, used or repurposed?

Typically, since the institution has collected (and maybe enhanced) the data, it is the owner of any IPR in that data. Notwithstanding IPR, the institution is also subject to the DPA. One key feature of the DPA is the right of an individual to have inaccurate data about them blocked or deleted, and this right over-rides any IPR ownership that the institution may happen to have over the data.

However, as noted earlier, as long as the personal data is created and processed in accordance with the DPA, the individual cannot object to its mere presence in the database. Under the DPA, any individual is entitled to receive a copy of the data pertaining to them, but if they do obtain a copy of such data, they should be aware that any IPR remains with the institution, so the individual might not be able to further reproduce or disseminate the data.

However, we might predict increasing interest in the value of activity data to the individual, especially if it becomes portable across personal and lifelong learning systems and wider social services such as recommenders. This is likely to raise issues regarding user rights to 'take away' their own data and on the other hand regarding any 'enhanced' data that may not be theirs to take, but which provides vital context to their data. Assuming IPR issues are surmountable, there will also be licensing choices as introduced below.

Further reading about this topic can be found here:

JISC Legal Information on IPR

http://www.jisclegal.ac.uk/LegalAreas/CopyrightIPR.aspx

Web2Rights project

www.web2rights.org.uk

Strategic Content Alliance IPR and Licensing Toolkit

www.web2rights.com/SCAIPRModule

http://sca.jiscinvolve.org/wp/allpublications/ipr-publications/

OER IPR Support Project

www.web2rights.com/OERIPRSupport

4.5 LICENSING FOR REUSE

The choice of data licences for facilitating reuse of anonymised activity data needs to take into account several key issues. Organisations need to balance their choice of reuse licences with their approach to "openness" and interopera bility; any possible third party rights issues and ensuing risks. They also need to consider their obligations under the Re-Use of Public Sector Information Regulations, which, whilst currently not applying to educational establishments, are likely to be a mended in the next couple of years.

Further resources about this topic can be found here:

Licensing Open Data: A Practical Guide

http://discovery.ac.uk/files/pdf/Licensing_Open_Data_A_Practical_Guide.pdf

Open Bibliographic Data Guide

http://obd.jisc.ac.uk/

Exploiting Activity Data

http://www.activitydata.org/index.html

Licensing compatibility

http://www.youtube.com/watch?feature=player_embedded&v=5BWqgVpcHCs

Re-Use of Public Sector Information Regulations

http://www.legislation.gov.uk/uksi/2005/1515/contents/made

4.6 LEGAL CONSIDERATIONS AT A GLANCE

The following tables summarise the key legal and ethical considerations.

Table 1 summarises these legal issue with reference to the main pieces of legislation and the related ethical issues.

Table 2 summarises the types of consequent risks associated with generating, using and sharing activity data and the types of actions that institutions might implement to mitigate such risks.

Table 1 - Legal Details and Ethical Implications

Issue	Legal Details	Ethical Implications
Data Protection	Data Protection Act 1998 [3].	Collection and Distribution; accuracy of data; right to view one's own data. Consent.
Freedom of Information	Freedom of Information Act 2000 [4].	The FoI Act does not permit passing of personal data, so there are no privacy threats.
Intellectual Property Rights	Copyright [5]. Database Rights [6].	Rights to my own data and the ability to access it for my own use.
Licensing	Customised data licences: Open Data Commons Licences [7]. Creative Commons Licences [8]. Open Government Licence [9].	Access to, control and reuse of my own data - lifetime portability. Lifespan and validity of use. Principles of reuse.

Table 2 - Risks and Mitigations

Issue	Risks	Mitigating Activities
Data Protection	Registration.. Responsibility.. Consent management.. Anonymity and traceability.	Data governance - developing clear organisational policies and procedures. Establishing organisational appetite for risk. Consent explicitly dealt with on opt in and / or opt out basis (below). Setting thresholds for group sizes (e.g. smaller than 20 represents higher risk).
Freedom of Information	Number and level of requests.	Developing clear organisational procedures and policies. Factoring expense of handling requests into budget.
Intellectual	Complexity.	Allocation of roles and responsibilities outlined in clear

Property Rights	Seeking permission and extent of any permissions granted. Understanding who has 'generated' activity data and any related terms. Other contractual obligations..	policies and procedures. Time and budget management. Seeking third party permissions where possible for any third party rights. Documenting permissions which have been granted in information management systems. Notice and Take Down Policy and Procedures for managing contested areas. [10]
Licensing	Who can the activity data be shared with and how? Expectation of "openness" and interoperability vs. potential commercial concerns. Ensuring that the data licence which facilitates sharing of the activity data is compatible with any third party rights and obligations associated with the activity data. Attribution stacking / lack of attribution.	Developing clear policies and procedures relating to organisational position on "openness". Establishing where the value lies and considering developing charged for services around the data. Understanding licensing as part of a holistic organisational approach to open licensing and commercial activities. Establishing an organisational licensing framework to help ensure that the selected data licence takes into account the extent of any permissions granted by third parties. Reconciling the need for attribution with optimising the interoperability of data.

5. Consent - Opt in or opt out?

Sharing personal data across and between institutions and service providers can be complex and will require compliance with legal responsibilities, particularly the DPA. Institutions need to understand the implications of the creation and dissemination of personal data, their roles and responsibilities regarding consent management, arising issues associated with anonymised data as well as the possible role of risk management decisions. A briefing paper by Naomi Korn and Professor Charles Oppenheim [11] provides more information on this topic as well as: a Risk Assessment Checklist and Good Practice Recommendations.

5.1 STRATEGIES

In a response to the potential extent of legal and ethical issues that might arise associated with the generation, use and sharing of activity data, UK universities and colleges need to discuss the merits and potential risks associated with consent and whether they adopt an opt in and / or opt out of their collection of student and staff activity data.

There are three plausible strategies that might be adopted:

- **Strategy 1** - initial opt in, (e.g. consent given at registration, or at the start of each academic year), still requiring further explicit opt in consent regarding any changes in policy and / or materials being collected.

- **Strategy 2** - initial opt in, (e.g. consent at registration), requiring only opt outs regarding any changes in policy and / or materials being collected.

- **Strategy 3** - initial opt out (e.g. at registration), requiring further opt outs regarding any changes in policy and / or materials being collected.

Each one may or may not be combined with the option for the individual to change their mind at any time during their involvement with the institution, or even after it.

5.2 RAMIFICATIONS

In order to comply with the principle of fair and lawful processing, the data controller should seek the consent of the person about whom data is being collected. The Data Protection Act 1998 does not specify whether opt-in or opt-out is to be used in any particular circumstances. Instead, it asks the wider question as to whether the user can be said to have given proper, informed consent. A confusing opt-out tick-box, with little or incomprehensible explanatory information is not likely to be considered as valid consent. Although an opt-in box is much more likely to be held to be consent, (as it requires a definite, positive action), the danger is that the user's inertia means failing to opt-in is a much higher risk.

The ICO has produced guidance on this, available at
http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/opt_in_out.aspx.

One exception applies where activity tracking is carried out using cookies. The latest Privacy and Communications Regulations (Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011) require prior consent before cookies are placed on the user's computer, though the latest ICO guidance allows for implied consent, provided there is sufficient information about the cookies to be used.

Higher Education and Further Education Examples

The following are examples of an opt-in approach to handling personalised data.

- Trinity College, Cambridge - http://www.trin.cam.ac.uk/show.php?dowid=934
- Homerton College, Cambridge -http://www.homerton.cam.ac.uk/pdf/data_protection_consent.pdf

We have no evidence of F/HE institutions offering an opt-out approach to individuals, though the principle has been adopted in other contexts.

- By UK government regarding the sale of personal data held in the Edited Electoral Register, which is permitted by law and presented as the default from which electors can opt-out on registration [12].
- Within the HE shared service supply chain – for example, by EDINA (OpenURL data – see 5.3 below).

5.3 SHARED SERVICES

A further variant of offering opt-in or opt-out options has been introduced by aggregation services (such as operated by EDINA and Mimas) and other shared services within the sector – though the same considerations would apply to aggregations performed outside the sector.

Within the sector, the work undertaken by EDINA, the JISC data centre at the University of Edinburgh, in running the shared OpenURL Router service and thereby collecting sector-wide activity data relating to e-journal access, provides a clear example. EDINA collects anonymised data relating to the activity of users from around 100 institutions, which it wishes to make openly available for analysis. It would be impractical to request permission of each user across the sector. Having taken legal advice, EDINA therefore gave each institution notice to opt-out of this value-added service, meaning that data from its users will be excluded. The implication in this cascade is that the institutions will have covered this type of collection and use in general yet adequate terms in their own local consent processes [13].

Beyond education sector boundaries, we should take account of how consumer services deal with multi-partner (shared, outsourced, etc.) issues relating to personal data and business intelligence. 'Business to Consumer' services increasingly involve extensive partnership arrangements within which personal data is transferred and processed. The education sector is increasingly involved in comparable arrangements precipitated by outsourcing and franchising. In Section 6, we explore how operations such as Amazon and Nectar deal with these supply chain requirements.

6. Ethical Dimensions

6.1 CONSIDERATIONS

In an interview with O'Reilly Radar [14] co-author Kord Davis of the forthcoming title 'Ethics of Big Data: Balancing Risk and Innovation' reflected that:

> 'Big data itself, like all technology, is ethically neutral. The use of big data, however, is not. While the ethics involved are abstract concepts, they can have very real-world implications. The goal is to develop better ways and means to engage in intentional ethical inquiry to inform and align our actions with our values. There are a significant number of efforts to create a digital "Bill of Rights" for the acceptable use of big data. The challenge is how to honor those values (transparency, security and accountability) in everyday actions as we go about the business of doing our work.'

In February 2012, the White House unveiled a blueprint for a Consumer Privacy Bill of Rights to protect consumers online [15]. As the President wrote in his cover letter to the report:

> "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times."

Given the education mission and associated corporate governance responsibilities, broad ethical considerations are crucial regardless of the compulsion in law. This impacts broad considerations and concerns about the use of personal data, as well as the specific uses involved in analytics.

- Type of data - principles for collection and use.
- Education mission - underlying issues of learning management, including social and performance engineering.
- Motivation for development of analytics – combination of corporate, individual and general good.
- Customer expectation – effective business practice, social data expectations, cultural considerations of a global customer base.
- Obligation to act – duty of care arising from knowledge and the challenges of student and employee performance management; this applies to things a student or employee may wish action to be taken on, and equally to things they may not. For example, a claim by a failed student that the institution should, through analytics, have predicted failure and therefore taken remedial action.

The following sections compare these considerations to existing models operating in the research, consumer and social network domains.

6.2 ETHICS AND RESEARCH PRACTICE

The Nuremberg [16], Helsinki [17], and Belmont [18] codes and guidelines provided the foundation of more ethically uniform research to which stringent rules and consequences for violation were attached. In 1946-47, in order to prosecute Nazi doctors for the atrocities they committed, a list of ethical guidelines for the conduct of research – the Nuremberg Code – were developed. The Nuremberg Code consisted of ten basic ethical principles, of which several are of strong relevance outside medical research and potentially apply to human data collected for analytics.

Nuremberg Code	Analytics in Post-compulsory Education	Relevance
Research participants must voluntarily consent to research participation.	Consent regarded as fundamental.	Strong relevance
Research aims should contribute to the good of society.	True of learning analytics but more complex in other areas that relate more explicitly to business success factors.	Some relevance
Research must be based on sound theory and prior testing.	Whilst initially experimental, data collection is underpinned by continuous testing of hypotheses in search of new narratives and actionable insights.	Weaker relevance
Research must avoid unnecessary physical and mental suffering.	The application of insights arising from learning analytics can cause suffering but not the research itself.	Strong relevance
Experiments can be conducted only by qualified persons.	The professionalization of ‘data scientist’ roles in IT teams and in domains such as teaching and learning and libraries is an essential aspiration.	Strong relevance
Subjects must be allowed to discontinue their participation at any time.	Unlike in the consumer world, it is perhaps hard to opt out and to ensure that your data will not be collected or used.	Some relevance

The Nuremberg Guidelines paved the way for the next major initiative designed to promote responsible research with human subjects, the Helsinki Declaration which lays out basic ethical principles for conducting biomedical research and has been revised and updated periodically since 1964. It contains the basic ethical elements specified in the Nuremberg Code but then advances further guidelines specifically designed to address the unique vulnerabilities of human subjects solicited to participate in clinical research projects. The next set of research ethics guidelines came out in the Belmont Report of 1979 from the US National Commission for the Protection of Human Subjects of Biomedical and Behavioural Research. The principles developed through these reports included the following:

Helsinki and Belmont	Analytics in Post-compulsory Education	Relevance
The importance of preserving the accuracy of research results and evidence based interpretation.	This is a core aspiration.	Strong relevance
The importance of determining which situations and conditions are appropriate and safe for research.	Appropriateness is a hard call though it will always be a headline consideration.	Strong relevance
Boundaries between practice and research.	The boundaries between research and practice are blurred in fast-moving fields such as learning analytics and recommender services; whilst there is little scope to conduct traditional research on a relevant scale, action research seems to be an essential rolling component of analytics strategy.	Weaker relevance
The principle of respect for persons, applied through informed consent.	This is fundamental; considerations include the duty of confidentiality.	Strong relevance
The principle of beneficence, applied through assessment of risks and benefits.	Risk assessment and benefits analysis is suitably engrained in HE operational practice; however practitioners may have an incomplete sense of the factors to be considered and also of the complexity and changing nature of the social systems in which they intervene.	Some Relevance

For further information

American Psychological Association principles and code of ethics

http://www.apa.org/monitor/jan03/principles.aspx

UK Data Archive

http://www.data-archive.ac.uk/create-manage/consent-ethics/legal

Institutional Example – University of Manchester

http://www.arts.manchester.ac.uk/postgraduatestudy/ethics/faq/

Does the collection of activity data in education differ from medical or general research?

Research ethics provide a valuable basis for thinking about the issues raised by analytics, with the added advantage of recognition within the educational community. However, the following table illustrates differences in terms of clarity of purpose and benefit.

Aspect	Research	Activity Data
Consent	Specific to the research or clinical episode.	Requires general acceptance that data will be collected.
Intent	Directed towards an agreed outcome.	May not be explicit, other than use within broad boundaries relating to personal benefit and business improvement.
Benefits	Both personal and global.	Corporate (business improvement), potentially personal (client experience), rarely sector wide or global.

6.3 BUSINESS AND CONSUMER PRACTICE

Where the collection of data for research purposes is governed by ethical and professional codes above and beyond legal obligation, the same processes in business are typically concerned simply with the letter of the law.

Clients in Further and Higher Education will typically be familiar with and accepting of (though perhaps not approving of) the practices of commercial organisations, whether online or on the street, such as retailers, advice and comparison services, and loyalty schemes.

- Mutuality of some kind is central to the relationship between the data collector and the data subject.
- Business and service improvement is an accepted intent.
- Direct client benefits may not be explicit but 'scheme benefits' can be an alternative 'sweetener' (e.g., loyalty points, membership offers, targeted recommendation, connection through data with a community).
- Consent is required but is typically as open-ended as possible.
- Wider partnership exploitation of the data is notified, sometimes but not always with an opt-out.
- Business are looking for new connections so they are collecting 'big data' (e.g., point of sale, click streams); 'just enough' data does not work.

Example - Nectar Card

http://www.nectar.com/help/privacyPolicy.nectar

The privacy policy for the multi-partner Nectar loyalty card is considered in the following table. The clarity is noteworthy:

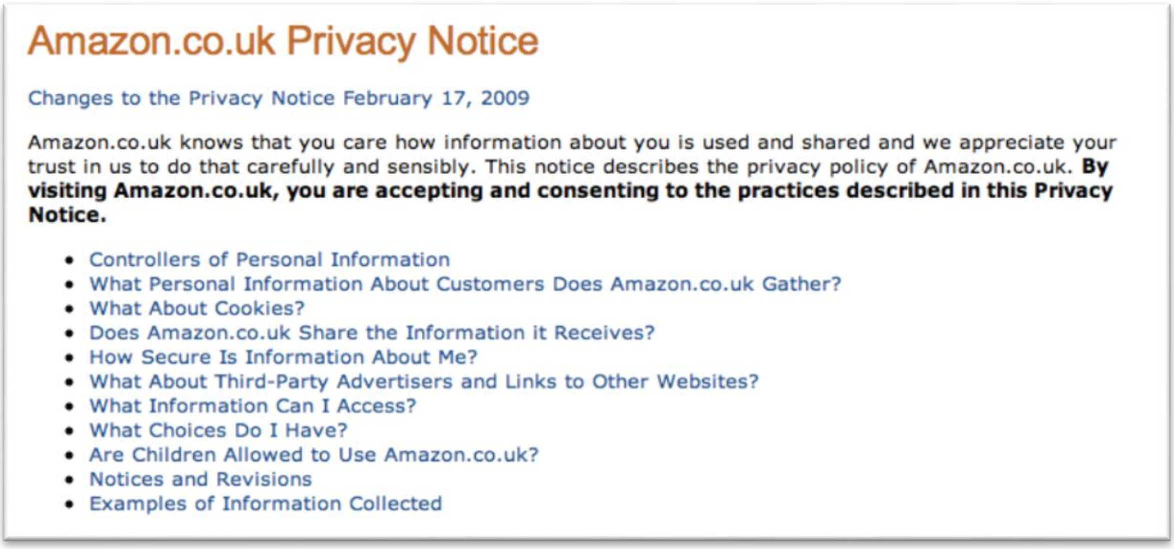
- This is about mutuality within the law rather than about ethical considerations, though recognised mutuality could be regarded as a strong ethical underpinning for such activity
- The involvement of named partner organisations is explicit.
- Acceptance of the approach is mandatory to join the scheme and thereby to enjoy the benefits.

Nectar Card Privacy Policy	Relevance to Analytics in Post-compulsory Education
What information will we use? By participating in Nectar, we will collect and use information about you and any additional collectors within your account. This information includes your registration details, information about the use of your Nectar card, shopping purchases and other information that you give us (together "your information").	This provides a template for a clear statement that can be mirrored in the institutional DPA registration.
How will your information be used? Your information may be analysed to see how you use the Nectar programme, to understand your shopping behaviour and to send you (and/or additional collectors on your account) information and offers for the products or services which are most likely to interest you. You agree to receive these communications in order to enjoy the benefits of participating in Nectar.	The intent and a degree of mutuality is explicit.
Who will we share your information with? We will only share your information within the Nectar group and with companies participating in Nectar and their group companies. A list of Nectar participating companies is available at http://www.nectar.com/about-nectar/legal/participating-companies.points.	There is a clear mechanism for acknowledging partners which could cover shared service, data centres and other outsourced services.
Links with Facebook are explicitly handled: http://www.nectar.com/about-nectar/legal/facebook.points By linking your Facebook account with your Nectar account, you agree to Nectar having access to and holding in accordance with Nectar's privacy policy: your Facebook 'basic information' (your Facebook user name, profile picture, gender, networks, user ID, list of Facebook friends and anything you have made public on Facebook); your email address held by Facebook; and information on what you 'like' on Facebook.	Recognition of the web of data sharing connections may be more problematic in education where initiatives may be system (e.g. VLE) or faculty specific; this raises data governance issues that would be less likely in a Business to Consumer (B2C) setting.

Example – Amazon.co.uk

Amazon UK also provides clear explanations about consent, security, the information collected (including the use of cookies), the involvement of third parties and the user's ability to access information about them (which only includes data directly entered, rather than tracking data).

The presentation of this policy information at http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=502584 offers a strong exemplar in terms of clarity and completeness (at least in the areas covered), as illustrated in the following screen image. The quality of explanation in itself may be argued to represent an ethical constructive approach.



Amazon.co.uk Privacy Notice

Changes to the Privacy Notice February 17, 2009

Amazon.co.uk knows that you care how information about you is used and shared and we appreciate your trust in us to do that carefully and sensibly. This notice describes the privacy policy of Amazon.co.uk. **By visiting Amazon.co.uk, you are accepting and consenting to the practices described in this Privacy Notice.**

- Controllers of Personal Information
- What Personal Information About Customers Does Amazon.co.uk Gather?
- What About Cookies?
- Does Amazon.co.uk Share the Information it Receives?
- How Secure Is Information About Me?
- What About Third-Party Advertisers and Links to Other Websites?
- What Information Can I Access?
- What Choices Do I Have?
- Are Children Allowed to Use Amazon.co.uk?
- Notices and Revisions
- Examples of Information Collected

Does the collection of activity data in education differ from good practice in the business to consumer world?

The practice adopted by leading business to consumer players provides a clear and legally grounded approach that is likely to be readily understood by the public in much of the world. In particular, the development of a sense of mutual gain, recognised and shared by a service organisation and its customers, is something to be learned from such as Amazon and Nectar.

Aspect	Business to Consumer	Education
Consent	General acceptance through broad based consent at registration; covering cookies and often providing clear exemplification.	Compatible with the B2C approach; there are lessons to learn from the level of explanation supporting the consent process.
Intent	To improve the business and its services.	Compatible with the B2C approach; whilst institutions way wish to be more expansive about benefits, this is not necessary and may carry risk.
Benefits	Typically linked to service improvement and / or loyalty schemes.	Whilst institutions may not be able to link loyalty schemes to activities such as learning analytics data collection, the core sense of mutuality is very strong.

From a broader UK society and government perspective, it is noteworthy that the data on the edited version of Electoral Register is available for purchase by law, now on an opt-out basis.

6.4 BRAVE NEW WORLD

It is suggested by some commentators that there is an imperative to review and even to revise ethical considerations on account of the increasingly widespread adoption and acceptance of:

- Online enquiry (e.g. comparison sites) and shopping with associated activity-based feedback loops.
- Social networking with its openness to making connections.
- Provision of preferences and automated use of activity data to filter information in order to save time.

Commentators such as Danish 'digital strategist' Peter Svarre [19] suggest new norms that arguably require a reinterpretation of our reservations, if not our ethical position. Svarre's presentation at the November 2011 OnTracks conference encapsulates this position [20].

This 'brave new world' perspective is based on the assumptions that;

- Successive generations of internet users are time poor whilst wishing to leverage an opportunity rich digital ecosystem.
- The 'born social' generation (one step beyond simply 'born digital') are positively accepting of the pros and cons of online identity and of such as automated association with 'people like me'.
- There is therefore a will, even a presumption of necessity, to trade privacy for other benefits within the new social economy.

An opposing position is taken up by Andrew Keen in 'Digital Vertigo' (subtitled 'How today's online social revolution is dividing, diminishing and disorienting us'). Keen presents an ethical crisis precipitated by the digital revolution, warning of the danger of 'collective self-destruction', including the loss of the rights privacy, autonomy and therefore liberty:

> But the problem is that, by so radically socializing today's digital revolution, we are, as a species, collectively jumping off a cliff. And if we fail to build a networked society that protects the rights to individual privacy and

> autonomy in the face of today's cult of the social, we can't ... launch a new company. Society isn't just another start-up – which is why we can't entirely trust Silicon Valley entrepreneurs like Hoffman or Stone with our future. Failing to properly assemble the social media airplane … means jeopardizing those precious rights to individual privacy, secrecy and, yes, the liberty that individuals have won over the last millennium.

More generally, a number of distinguished authors such as Jaron Lanier ('You are not a Gadget: a Manifesto'), Eli Pariser ('The Filter Bubble: what the Internet is hiding from you') and Evgeny Morozov ('The Net Delusion: How not to liberate the world') have pointed to the personal and societal downsides of an online data-driven culture.

The position presented by Keen, speaks deeper to the human condition and a Jeffersonian protection of inalienable rights than more immediate considerations of consent, the client comfort zone or the value of lifelong personal data ownership.

Even if we regard Keen's position as alarmist, institutions will be aware of challenges presented by the attitudes of some supply chain partners in their attitudes to the collection of such as activity data, which seems far from benign or collaborative. The barriers erected by publishers (e.g. resistance to sharing publicly article level access data) are a recurrent but far from isolated example.

6.5 DOES DOMAIN OR APPLICATION MAKE A DIFFERENCE?

There is danger in assuming that ethical considerations are universal and therefore promoting the transferability of norms across cultural and domain boundaries – in this case adopting the norms established about the use of personal data for analytical purposes in other domains as explored above (research, consumer services and social networks).

In 'Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy' [21], political philosopher Jurgen Habermas argues that in a modern pluralist culture normative issues should be separated from issues of the good life. Only when various ethical traditions come into conflict with one another, as they inevitably do in a modern pluralist culture, do normative issues arise that have implications for everyone.

It is argued therefore that ethical norms are defined by discourse in particular communities of practice. For example, the public now has a general understanding of these such that when they come across medical research they know what to expect, and equally know that B2C services have a different ethical stance, whilst both operate within the law. Meanwhile new fields of activity such as education analytics lack convention and operationalisation of ethical principles, understanding about what is actually going on and where the line is drawn in grey areas and perhaps also the defining stereotypes that catalyse norms, as witnessed at Nuremberg.

So the challenge is whether the education community, not least in the emerging field of learning analytics, should revise its ethical position on account of the widespread changes of attitude in the digital realm from which learners and researchers are increasingly drawn. At the very least, even if ethical norms are not immutable, their current application in terms of self-evident good practice provides candidates for adoption regardless of context. This is exemplified in the norms of medical and research ethics and B2C services introduced above.

Finally, regarding the development of norms, we may need to distinguish between differing uses of analytical data within the core educational mission, taking care to assess whether the same principles and practice apply to the different applications. Consider, for example, the different classes of teaching and learning application set out in the April 2012 US Department of Education learning analytics report [22]:

- The report identifies purposes directly geared to benefit the close-to-real-time learner experience: user profiling, adaptation and personalisation, user knowledge and behaviour modelling, and user experience modelling.

- It also highlights systemic or process improvement purposes to which the same analytical data can be applied: domain modelling, learning system component analysis, instructional principle analysis, and trend analysis.

6.6 GUIDING PRINCIPLES

As Voltaire's Candide might have reflected, we are faced with the imperative to seek out the 'best of all possible worlds':

- **In assuring educational benefits**, not least supporting student progression, maximising employment prospects and enabling personalised learning (i.e. in the specific domain of learning analytics), it is incumbent on institutions to adopt key principles from the research ethics, as enumerated in 4.1 above.

- **As businesses**, post-compulsory educational institutions are facing the same business drivers and globalised competitive pressures as any organisation in the consumer world, as exemplified in 4.2 above.

- **To satisfy expectations** of the born digital / born social generations, there is a likely requirement to take on new ethical considerations, which may run contrary to the sensibilities of previous generations, especially in respect of the trade-off between privacy (as opposed to confidentiality) and service, as examined in 5.3 above. Furthermore we might anticipate these expectations to be sharpened by increased fees.

We suggest that there are common principles that provide for good practice above the level of these apparent conflicts:

- **Clarity** – definition of purpose, scope and boundaries, even if that has to recognise it is broad and in some respects open-ended.

- **Comfort and care** – consideration for both the interests and the feelings of the data subject and vigilance regarding exceptional cases (for example, regarding alleged infringement of privacy or unsolicited advice).

- **Choice and consent** – opportunity to opt-out / opt-in and to withdraw (which may involve withdrawing from the wider entity, such as the university).

- **Consequence and complaint** – recognition that there may be unforeseen consequences arising from handling of such data and therefore providing mechanisms for complaint and take-down.

7. References

1. http://www.jisc.ac.uk/blog/no-such-thing-as-a-free-mooc/

2. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

3. http://www.legislation.gov.uk/ukpga/1998/29/contents

4. http://www.legislation.gov.uk/ukpga/2000/36/contents

5. http://www.ipo.gov.uk/cdpact1988.pdf

6. http://www.ipo.gov.uk/cdpact1988.pdf

7. http://opendatacommons.org/

8. www.creativecommons.org

9. www.nationalarchives.gov.uk/doc/open-government-licence/

10. http://sca.jiscinvolve.org/wp/portfolio-items/briefing-paper-on-managing-orphan-works-2/ and http://sca.jiscinvolve.org/wp/portfolio-items/template-notice-and-take-down-policy-and-procedure/

11.http://www.jisclegal.ac.uk/Portals/12/161111%20Consent%20Management%20Briefing%20Paper.pdf. This paper is based on a more comprehensive report by JISC Legal "Consent Management: Handling Personalisation Data Lawfully" - http://www.jisclegal.ac.uk/Themes/IdentityManagement.aspx

12. http://www.ico.gov.uk/for_the_public/topic_specific_guides/electoral_register.aspx

13. The investigation undertaken by the University of Edinburgh is covered at http://edina.ac.uk/projects/Using_OpenURL_Activity_Data_Initial_Investigation_2011.pdf

14. http://radar.oreilly.com/2012/06/ethics-big-data-business-decisions.html

15. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

16. http://en.wikipedia.org/wiki/Nuremberg_Code

17. http://en.wikipedia.org/wiki/Declaration_of_Helsinki

18. http://en.wikipedia.org/wiki/Belmont_Report

19. http://www.petersvarre.dk/

20. http://ontracks.dk/

21. http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=8386

22. http://evidenceframework.org/wp-content/uploads/2012/04/EDM-LA-Brief-Draft_4_10_12c.pdf

About the Author

David Kay is a senior consultant at Sero Consulting Ltd (http://www.sero.co.uk). He joined Sero in 2004 after over 20 years involvement in the design and development of IT systems for education and library management and for learner support.

David began investigating the potential of activity data and resulting analytics in connection with Higher Education libraries in the 2009 JISC TILE project, working with Mark van Harmelen (Hedtek) and Ken Chad. He has subsequently been involved in JISC's further examination of those concepts in the MOSAIC demonstrator project and in the University of Manchester synthesis of the 2011 Activity Data programme (http://activitydata.org).

CETIS Analytics Series

Vol.1 No.1. Analytics, What is Changing and Why does it Matter?
Vol.1 No.2. Analytics for the Whole Institution; Balancing Strategy and Tactics
Vol.1 No.3. Analytics for Learning and Teaching
Vol.1 No.4. Analytics for Understanding Research
Vol.1 No.5.What is Analytics? Definition and Essential Characteristics
Vol.1 No.6. Legal, Risk and Ethical Aspects of Analytics in Higher Education
Vol.1 No.7. A Framework of Characteristics for Analytics
Vol.1 No.8. Institutional Readiness for Analytics
Vol.1 No.9. A Brief History of Analytics
Vol.1 No.10. The Implications of Analytics for Teaching Practice in Higher Education
Vol.1 No.11.Infrastructure and Tools for Analytics
http://publications.cetis.ac.uk/c/analytics

Acknowledgements

The CETIS Analytics Series was commissioned by Myles Danson (JISC programme manager) to give an overview of current thinking around analytics in post-16 education in the UK. In addition to the authors the following people have contributed to the production of the CETIS Analytics Series; Lorna Campbell (CETIS), Adam Cooper (CETIS), Rob Englebright (JISC), Neil Jacobs (JISC), Sheila MacNeill (CETIS) and Christina Smart (CETIS). Design and Artwork by: http://www.consul4design.com

About this White Paper

Title: Vol.1 No.6.: Legal, Risk and Ethical Aspects of Analytics in Higher Education

Authors: David Kay (Sero Consulting), Naomi Korn and Professor Charles Oppenheim

Date: November 2012

URI: http://publications.cetis.ac.uk/2012/500

ISSN 2051-9214

Published by The University of Bolton

About CETIS

CETIS are globally recognised as leading experts on interoperability and technology standards in learning, education and training. We work with our clients and partners to develop policy and strategy, providing impartial and independent advice on technology and standards. CETIS are active in the development and implementation of open standards and represent our clients in national, European and global standards bodies and industry consortia, and have been instrumental in developing and promoting the adoption of technology and standards for course advertising, open education resources, assessment, and student data management, opening new markets and creating opportunities for innovation.

For more information visit our website: http://jisc.cetis.ac.uk/

The Analytics Series has been produced by CETIS for JISC: http://www.jisc.ac.uk/