Research in Learning Technology
Vol. 27, 2019

ORIGINAL RESEARCH ARTICLE

Non-institutional learning technologies, risks and responsibilities: a critical discourse analysis of university artefacts

Sam Berry*

Swansea University Medical School, Swansea University, Swansea, UK

(Received: 14 June 2019; Revised: 2 October 2019; Accepted: 15 October 2019; Published: 21 November 2019)

Non-institutional technologies include external or third-party technologies that are not officially sanctioned or supported by higher education institutions (HEIs) but may be used by staff for educational purposes. These include free, open-source and open-access technologies such as social media sites, apps and online services. The literature identifies a number of risks and ethical considerations when using digital technologies, such as security, safety, privacy and legal compliance (Common Sense n.d.). This study analyses institutional artefacts, including policy and guidance documents, to explore how institutions are addressing the risks of educational technologies identified throughout the literature.

Critical discourse analysis was conducted on nine artefacts, obtained from seven UK HEIs. The study found that institutional policies and guidance documents do not sufficiently address some of the key risks identified in the literature (e.g. security risks), nor consider the ethical issues emerging from the use of profit-making educational products. Users of these technologies (including teaching staff) are assigned a broad range of complex and potentially time-consuming responsibilities concerning the evaluation, selection and operation of these technologies. For example, to ensure compliance with data protection legislation, however, no artefact stated how this should be achieved. The study therefore identifies significant inadequacies in institutional policies and guidelines, and questions whether appropriate quality assurance processes and safeguards are in place when non-institutional technologies are used for higher education.

Keywords: third party; security; privacy; data protection; policy

Introduction

There has been increasing development and availability of open-access, open-source and free online services that can be used by learners and educators, i.e. a decentralised technology model (Weller 2010). There are a number of benefits of these technologies such as scalability, familiarity and cross-platform compatibility (Conole and Alevizou 2010). There are also risks and considerations. For example, what mechanisms are in place to protect learners' data when stored in the cloud? Is it appropriate to use an educational app if the app collects personal data from students' devices or sells that data? To what extent are teaching staff responsible for answering these questions, when the technology is not institutionally provided or supported?

*Corresponding author. Email: s.berry@swansea.ac.uk

Citation: Research in Learning Technology 2019, **27**: 2284 - http://dx.doi.org/10.25304/rlt.v27.2284

This study evaluates institutional artefacts which relate to the use of non-institutional technologies by teaching staff for educational purposes. The emphasis on educational purposes intends to distinguish this from other potential uses within academia, such as to conduct or disseminate research. Although this study does not focus on how these artefacts are implemented in practice, this study intends to make a contribution to the field by exploring the extent to which higher education institutions (HEIs) consider risks and ethical issues, and the standards and procedures set out to address these issues when non-institutional technologies are adopted by staff for educational purposes. Document analysis can also contextualise empirical findings, and suggest areas for further investigation (Bowen 2009).

Research questions

RQ1: How do institutional texts distinguish between institutional and non-institutional technologies?

RQ2: According to these texts, what responsibilities are assigned to teaching staff when non-institutional technologies are utilised for educational purposes?

RQ3: According to these texts, to what extent do teaching staff have autonomy to use non-institutional technologies?

Literature review

Technology risk in higher education

There are many examples in the literature of the various ways that digital technologies are being used to support learning, teaching and assessment within higher education. For example, this might include students using a mobile device to participate in a live poll (Shon and Smith 2011), using WhatsApp to facilitate learning whilst on placement (Raiman, Antbring, and Mahmood 2017), or maintaining an ePortfolio for assessment (Garrett, MacPhee, and Jackson 2013).

Security and privacy issues have been identified and widely reported concerning educational technologies (e.g. Alim *et al.* 2017; Kelly *et al.* 2018; Kelly, Graham, and Fitzgerald 2018; Lorenz, Kalde, and Kikkas 2012). There are many threats to educational systems beyond deliberate and malicious attacks, such as accidental data loss, data corruption and loss of service (due to upgrade interruption or through discontinuation) (Akande and Van Belle 2016). Online and cloud-based services also pose a number of considerations, such as whether it is appropriate for third-party service providers to be able to access confidential and sensitive data that may exist if these services are being used for educational purposes. This could include the student's personal details (such as name and email address), demographic information, learning and assessment data (such as grades, feedback, failures and attempts) and information concerning special circumstances or specific learning difficulties (Regan and Jesse 2018). In addition, Polonetsky and Tene (2014) report that online educational services surreptitiously collect data using passive methods such as cookies. Passive data collection occurs through the use of a device or application, and can be used to continuously capture data such as location and movement tracking, activity data (such as search history) and emotional data (Herold 2018), which may occur without the user's knowledge or informed consent, and even when a device or application is not in use (Brandtzaeg, Pultier, and Moen 2018).

Some UK HEIs have developed 'bring your own device' (BYOD) policies (Walker *et al*. 2014), which may require staff and students to access educational services and applications from personal devices (Chatzigavriil *et al*. 2014). Security, privacy and data protection issues are therefore of particular concern given the wealth of personal data that may exist on or be generated from personal devices (Miller, Voas, and Hurlburt 2012). There are also a number of ethical issues to consider concerning the use of profit-making online tools (Purvis, Rodger, and Beckingham 2016), which can collect and disseminate personal data for advertising firms to exploit (Lindh and Nolin 2016), or who may share or sell users data or content (Kelly *et al*. 2018b).

Previous studies have found that students are concerned about their online privacy when using digital technologies in higher education (Aymerich-Franch and Fedele 2014). Students' perceptions of security and privacy can influence the educational use of cloud-based technologies (Arpaci, Kilicer, and Bardakci 2015) and their participation in online learning (Lorenz, Sousa, and Tomberg 2013). Furthermore, a previous study found that students assumed and expected their tutors and/or the institution to have conducted checks (such as for malware) prior to recommending or requesting the use of third-party educational technologies (Author 2019). Hardré (2016) has asserted that when individuals believe that someone or something else is observing or monitoring a situation, they become subconsciously less watchful of it themselves, i.e. there is diminished vigilance. There is therefore the risk that if students expect someone else to have performed checks and implemented safeguards, that they assume these products are trustworthy and safe, and do not take precautions themselves e.g. reading the terms and conditions. Furthermore, it has been argued that when risks are imposed without consent, they may be considered less acceptable than when undertaken voluntarily (Farahmand, Yadav, and Spafford 2013).

However, conducting such checks would require technical and legal knowledge. Privacy statements have been criticised for being verbose and containing technical or vague terms that are difficult to understand (Reidenberg *et al*. 2015). Furthermore, there are limitations to the checks that can be conducted by end users as it is unlikely that access to information or systems would be available to conduct comprehensive evaluations. For example, how might an individual check for the presence of malware prior to downloading a product?

Higher education policy on technology use in teaching and learning

Conole (2013) asserts that there needs to be a balance between institutional coordination and individual experimentation with digital technologies. This requires the need for clear policies and guidelines (Conole 2013). Within this study, a policy is defined as '…administrative regulation …used to define the obligations of the institution, expectations of employees and/or students, and consequences if the expectations are violated' (Lenartz 2012, p. 346).

A literature search was conducted on 10th April 2017, using Scopus, to identify the literature on UK HEI policies, regulations or guidelines, and the use of non-institutional technologies. The following search terms were used:

> (higher education) AND (UK)
> AND
> (external AND services) OR (third AND party) OR (cloud) OR (web 2.0) OR (outsource*) OR (non-institutional)

AND
(polic*) OR (regulation*) OR (guidance) OR (guidelines) OR (strateg*) OR (best AND practice)

The search generated 26 results, none of which were found to be relevant to this study. Similar studies were found through conducting further searches on Scopus and Google Scholar. These included an evaluation of social media policies (McNeill 2012; Pomerantz, Hank, and Sugimoto 2015), copyright of eLearning and teaching materials (Gadd and Weedon 2017), eSubmission (Newland, Martin, and Ramsden 2011) and the electronic management of assessment (Voce 2015). In a similar study, Pomerantz, Hank, and Sugimoto (2015) reported that as of 2015, there is only one study that has assessed the content of social media policies. This demonstrates that there is a lack of empirical and theoretical work in this area. Furthermore, studies that focus on policies may be limited, as there are many types of institutional documentation, such as contracts, information guides and staff training materials that can also establish and promote institutional expectations, quality standards and employee responsibilities.

Research design

Methodology

Within this study, a social constructivist view is taken, in which the language of institutional texts '…does not describe social processes and structures, but creates and supports them' (Saarinen 2008, p. 719). One limitation of this study is that it will not investigate the perspectives or experiences of individuals. However, these texts are seen as ways in which institutions represent and account for themselves (Coffey 2014), promote and constrain particular practices and provide an insight into the conditions that can have an impact upon the phenomena under investigation (Bowen 2009).

Discourse is considered to play a significant role in the creation and shaping of social processes (Saarinen 2008). Critical discourse analysis (CDA) is both an analytical tool and a theoretical approach, which emphasises making the hidden visible (Saarinen 2008); therefore, CDA can be used to interrogate texts to explore how social relations are reproduced or contested, assess whose interests are served or negated, how the text is positioned or positioning and explore the consequences of this positioning (Janks 1997).

Method

Document analysis is a systematic procedure for reviewing or evaluating documents (Bowen 2009). Within CDA, there is no set procedure to generate a sample (or corpus) for evaluation, as '…people approach it in different ways according to the specific nature of the project, as well as their own views of discourse' (Fairclough 1993, p. 225). The lack of literature in this field means that the type of artefacts to be collected and the prevalence of those artefacts are unknown. Therefore, 30 UK HEIs (18%) were randomly chosen from the list of 167 UK HEIs, produced by HESA. The purpose of the sampling exercise was not to generate a statistically representative sample, but an analytically diverse sample. Ethical approval for this study was granted on 9th March 2017, by a Higher Education Research Ethics Committee.

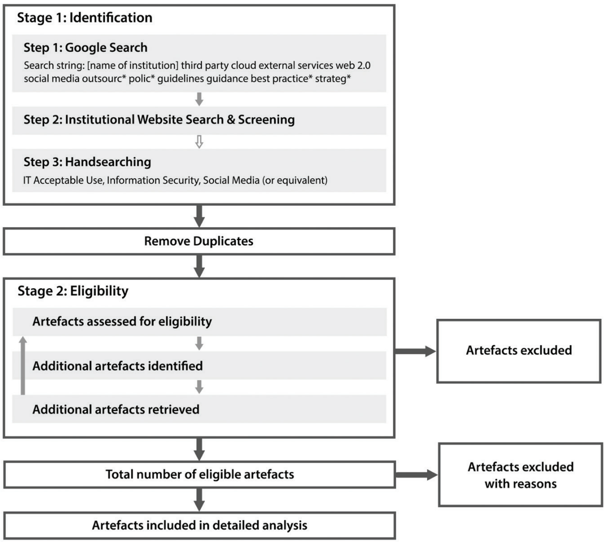
Stage 1: Identification
Step 1: Google Search
Search string: [name of institution] third party cloud external services web 2.0 social media outsourc* polic* guidelines guidance best practice* strateg*
Step 2: Institutional Website Search & Screening
Step 3: Handsearching
IT Acceptable Use, Information Security, Social Media (or equivalent)
Remove Duplicates
Stage 2: Eligibility
Artefacts assessed for eligibility
Additional artefacts identified
Additional artefacts retrieved
Artefacts excluded
Total number of eligible artefacts
Artefacts excluded with reasons
Artefacts included in detailed analysis

Figure 1. A summary of the research process.

A scoping exercise was conducted using Google Search and HEI websites to explore artefacts that may be relevant to this investigation and generate search criteria. This informed the development of a process outlined in Figure 1. The PRISMA 2009 Flow Diagram (Moher *et al*. 2009) inspired the development of this process, namely in terms of providing a systematic framework in which to organise the data collection phases.

Stage 1 was conducted for each institution, and upon completion, all artefacts were reviewed for eligibility (stage 2) based on three key factors:

1. The intended audience must include teaching staff (whether explicitly stated or implied).
2. The artefact must include non-institutional technologies.
3. The artefact must include educational purposes.

It is recognised that this process is not exhaustive and that alternative steps could have been taken by contacting the institutions or organisations such as the Heads of eLearning Forum (as has been conducted in previous HE policy studies such as Newland, Martin, and Ramsden 2011). However, the benefit of conducting the study this way is that it intends to not limit the artefacts to those produced by particular communities within the institution, or to particular genres of discourse.

CDA was conducted on a subset of the eligible artefacts retrieved (as explained in the following section). A framework was produced to guide the analysis process based on the work of Fairclough (2001), Boag-Munroe (2004), O’Connell (2015) and Voce (2015)**.** The framework was organised into structural and linguistic factors for analysis, such as interdiscursivity, accessibility, speech functions, grammatical mood and modality. These areas of analysis were prioritised based on their relevance to the research questions. Speech functions can signal the authors commitment to truth (epistemic modality) and the authors commitment to obligation or necessity (deontic modality) (Fairclough 2003). Modality can be used to determine the authors ‘degrees of affinity’ to the proposition (Fairclough 1993), and can therefore signify the institutions commitment to propositions, and the level of authority present within the texts (Voce 2015).

Data analysis

Data collection was conducted on April 2017. Figure 2 summarises the number of artefacts found and reviewed at each stage.[1] Artefacts were obtained for 25 (83%) of the institutions as a result of stage 1. For the remaining institutions, it is possible that relevant artefacts may not be publicly available.

Assessing the eligibility of the artefacts was very difficult, given the range of texts and limitations of interpretation as an outsider. For example, a number of artefacts were found relating to the use of external or cloud-based services but did not explicitly reference educational uses of these technologies or were unclear on whether the text applied to teaching staff. Each of the documents reviewed in stage two (n = 100) were assigned a colour (shades of blue), which signified the degree to which it aligned with the eligibility criteria. The stronger the colour, the greater the relevance to this study (summarised in Table 1).

A total of 29 artefacts were excluded upon completion of stage 2, either because they did not meet the eligibility criteria (n = 27, marked in grey in Table 1) or because it was not possible to determine whether they applied to teaching staff (n = 2, marked in orange).

A total of 71 artefacts (from 22 institutions) were retrieved which related (to some degree) to the use of non-institutional technologies within HEIs. However, to facilitate an in-depth CDA of these texts, the nine most relevant artefacts (from seven institutions) were selected, eight documents and one website. Table 2 provides an overview

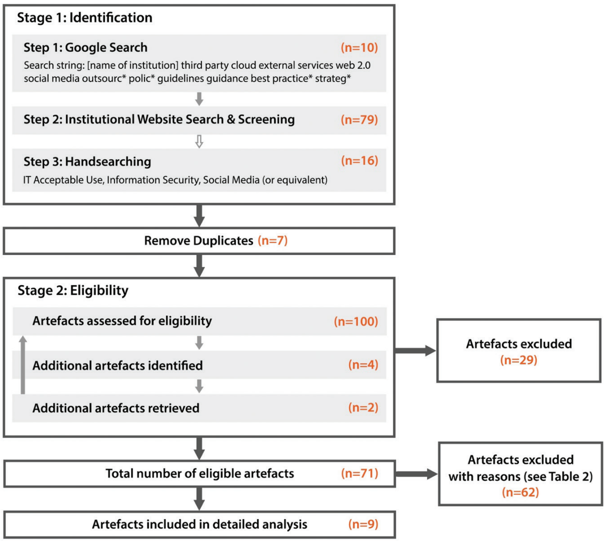
Stage 1: Identification
Step 1: Google Search
(n=10)
Search string: [name of institution] third party cloud external services web 2.0 social media outsourc* polic* guidelines guidance best practice* strateg*
Step 2: Institutional Website Search & Screening
(n=79)
Step 3: Handsearching
(n=16)
IT Acceptable Use, Information Security, Social Media (or equivalent)
Remove Duplicates (n=7)
Stage 2: Eligibility
Artefacts assessed for eligibility
(n=100)
Additional artefacts identified
(n=4)
Additional artefacts retrieved
(n=2)
Artefacts excluded
(n=29)
Total number of eligible artefacts
(n=71)
Artefacts excluded with reasons (see Table 2)
(n=62)
Artefacts included in detailed analysis
(n=9)

Figure 2. A summary of the research process.

[1] Note that for copyright reasons and to preserve anonymity, quotations could not be reproduced from these artefacts. Instead, the examples presented throughout are fabricated, but based on actual statements.

Table 1. Summary of the eligibility score for each institutional artefact reviewed.

Institution No.	Eligibility score	Institution No.	Eligibility score	Institution No.	Eligibility score	Institution No.	Eligibility score
I01	▣	I07	▧	I13	□	I21	▦
	▦		▤		▦		□
	□		□		🟧		▦
	▤		▦		▨		▦
	□		▨		▨	I23	□
	□	I09	▨		▨		■
	▨		▨	I15	□	I24	🟧
	▨		▨		▤	I25	■
I02	▨		□		▦		▦
	▦		□		□		▨
	▨		▨	I16	□		▨
	▨		□		□	I27	□
	□	I10	□		□		■
	▨		□		■		□
	▣		▦	I17	▨		■
	□		▨		▨	I28	▦
I04	▦	I11	■	I18	▦		□
	▨		□		□		▨
	▨	I12	▦		▨	I29	▦
	▦		□	I19	▦		□
	□		□		□	I30	▦
	▣		▦	I20	▦		▨
	▣		□		□		■
I05	▨		▣				□
	▨		▣				▦
I06	▦		□				

Table 2. HEI mission group affiliation and student numbers (HESA n.d.).

Institution No.	Mission Group	No. Students0
I04	University Alliance	20000 -< 25000
I11	Unaffiliated	5000 -< 10000
I16	University Alliance	20000 -< 25000
I23	Million+	10000 -< 15000
I25	Unaffiliated	5000 -< 10000
I27	Guild HE	5000 -< 10000
I30	Unaffiliated	10000 -< 15000

Note: Please note that the precise number of students is not provided to preserve anonymity.

of the HEIs included in the study, and Table 3 summarises the production details for each artefact.

There was great variation in the tone of the artefacts. Artefacts 3, 5 and 8 (policy documents) were more formal in tone, signified by institutional logos, publication details, structure (e.g. numbered headings and sub-headings), lexical choice and declarations. For example, A5 declared that it was a mandatory policy. In contrast, artefacts 1, 2 and 9 were less formal, and A1 was more collegial in tone. Artefacts 4–7

Table 3. Production details for each artefact.

Artefact No.	Artefact type	Publication date	Review date	Version number	Author/s	Production information	Length (words)
A1	Guidelines – use of external services or software for learning	No	No	No	Unknown	Learning and Teaching Committee	792
A2	Staff induction document – learning technologies	No	No	No	Unknown		110
A3	Acceptable use policy	2014	2016	2.0	Individual (Information Services and Technology Dept.)		3978
A4	Social media policy	No	No	No	Educational Development Unit		1563
A5	Social media policy	2015	N/A	1	Unknown	Legal, Digital Services, Information Security & Policies Committee	3883
A6	Social media policy	No	No	No	Unknown	Individual (Marketing Department)	4436
A7	Social media guidelines	No	No	No	Unknown		2381
A8	Social media policy	2012	N/A	No	Unknown	Marketing	1442
A9	Social media: staff user guide (website)	No	No	No	Unknown	Marketing and Student Recruitment	3676

were inconsistent in tone. For example, A6 used both formal and informal language in different parts of the document.

Each sentence (including bullet points) was analysed and thematically coded through an iterative deductive process. If a sentence related to multiple themes, the sentence was separated into thematically distinct phrases. Table 4 is an overview of the themes and frequency of occurrence, i.e. the number of phrases or sentences.

Rules (including guidelines) took the form of *commands* (i.e. assigned actions and/or responsibilities), *restrictions* (i.e. prohibited activities), *boundaries* (i.e. defined concepts and/or responsibilities), *monitoring activities* and the *consequences* for non-compliance. Commands were the most predominant form of rule in each of the artefacts, and were expressed with the speech function of demand, a form of deontic modality which signifies the '…"author's" commitment to obligation [or] necessity' (Fairclough 2003, p. 168). Commands were articulated in one of the following ways (based on Fairclough 2003).

- Prescriptions, usually positive imperative clauses, e.g. 'Complete a risk assessment'.
- Proscriptions, usually negative imperative clauses, e.g. 'Do not post anonymously or use pseudonyms'.
- Modalised demands, which lie between prescriptions and proscriptions, and may contain markers such as modal verbs, e.g. 'Staff must adhere to the Data Protection Act'.
- Interrogative demands (i.e. question-requests), e.g. 'Does the learning tool comply with accessibility standards?'
- Statements with deontic modality, e.g. 'All University social media activities are subject to UK Legislation'.

Figure 3 summarises the format and number of commands for each of the artefacts.

Two types of modal markers were analysed: modal verbs and participial adjectives (namely 'required', 'supposed' and 'allowed'). However, participial adjectives were seldom used. Using the Halliday and Matthiessen's (2013) modal classification model, the level and frequency of modal verbs were analysed, as summarised in Table 5. This was to analyse the level of authority present within the texts which can indicate the level of compliance required. The colours in the table highlight the level of modulation most frequently used within each of the artefacts, with A7 and A8 (from the same institution) containing the greatest use of high-level modal verbs.

All phrases/sentences relating to commands, restrictions and boundaries (CRB) were analysed and thematically coded. A very broad range of themes were prevalent across the artefacts, as evidenced in Table 6. The total frequencies present a skewed perspective as each of the artefacts varies greatly in length. Therefore, the most frequent CRB category is highlighted for each artefact, demonstrating two important findings. Firstly, the artefacts vary in terms of the breadth of CRB themes included within the texts, with some artefacts focussing more on some areas than others. For example, artefact A3 (acceptable use policy) contained more statements relating to security, malicious acts (i.e. purposeful malicious behaviours such as distributing viruses) and password management than A1 (guidelines on the use of external software/services for learning) which contained more statements relating to data protection and the selection of technologies. Secondly, the table reveals themes that are

Table 4. Content themes and frequency.

Theme		A1	A2	A3	A4	A5	A6	A7	A8	A9	Total
Purpose (of the artefact)		3	0	4	2	3	4	2	1	1	**20**
Encouragement (to use technologies)		2	0	2	2	1	1	0	0	0	**8**
Benefits (of technologies)		5	0	2	6	2	2	6	1	3	**27**
Risks (of technologies)		1	0	8	2	2	1	8	0	1	**23**
Rules	Commands	20	1	63	41	80	77	57	27	47	**413**
	Restrictions	1	2	9	1	5	7	3	2	10	**40**
	Boundaries	0	0	1	5	15	3	7	4	1	**36**
	Monitoring	0	0	5	1	3	8	3	0	0	**20**
	Consequences	0	0	5	2	4	4	0	1	0	**16**
Technical Restrictions		0	0	2	0	0	0	0	0	0	**2**
Interests		3	1	9	5	18	5	6	2	2	**51**
Sources of Support/Guidance		5	1	2	1	9	5	2	6	15	**46**
Total		**40**	**5**	**112**	**68**	**142**	**117**	**94**	**44**	**80**	**702**

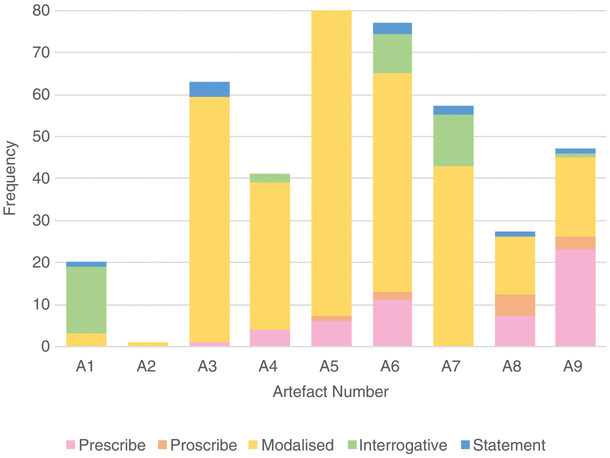

Figure 3. Linguistic style of commands.

Table 5. Frequency of modal verbs.

	A1	A2	A3	A4	A5	A6	A7	A8	A9	Totals
High *(must,ought to, need to,)*	1	0	18	5	29	11	31	90	2	**106**
Median *(will, would, should, shall)*	8	0	35	29	42	45	20	8	15	**202**
Low *(could, can/not, may, might)*	7	1	22	8	24	31	25	6	15	**139**
Total	**16**	**1**	**75**	**42**	**95**	**87**	**76**	**23**	**32**	**447**

absent within the artefacts. For example, only artefacts A1, A4 and A8 refer to accessibility requirements.

Discussion

How do institutional texts distinguish between institutional and non-institutional technologies?

No artefact explicitly defined nor stated the distinguishing characteristics between institutional and non-institutional technologies. Definitions were provided for the term ‘social media’ in artefacts A4, A5, A6 and A8; however, no distinction was made between institutional and non-institutional social media tools (such as discussion forums and blogs on institutional Virtual Learning Environments (VLEs)). Artefact A1 was a dedicated guidance document on the use of external services or software for learning, but did not define ‘external’. The artefact included a link to a list of ‘provided’ software and services, implying institutional technologies, although the page was no longer available.

Verbs were analysed for any related phrases, revealing that the terms maintained, provided, owned, offered, approved and administered were used in reference to internal, central or university technologies, i.e. institutional technologies. The term ‘external’ was used in relation to technologies in five artefacts (A1, A2, A3, A6 and A7), which implies non-institutional technologies, and the terms ‘hosted’ and ‘not supported’ were used in association with these technologies.

Table 6. Frequency of commands, restrictions and boundaries (CRB), categorised by theme.

	Artefact No.									
Theme	A1	A2	A3	A4	A5	A6	A7	A8	A9	Total
In/Appropriate Use/Conduct/Content	1		8	7	27	26	10	10	16	**105**
Account/Content Mgmt				8	9	13	3		9	**42**
Moderating and Responding				2	6	11	5	1	8	**33**
Data Management (incl.backup)	3	1	6	2	1		3			**16**
Data Protection	4		3	4	5	2	12	3		**33**
Privacy	1		1	2	9	3	6	7		**29**
Security (general)			16		1	1	4	1	1	**24**
Password Management			9		2					**11**
Confidentiality			1		3	1	2	1		**8**
Malware			7							**7**
Spam					1		1			**2**
Comply with Policies			8	8	7	4	3	4	1	**35**
Copyright and IPR			1	2	13	1	3	3		**23**
Comply with Legislation	1		2	2	2	3	2			**12**
Freedom of Information				1	1					**2**
Aims/Purpose	2			2		2	3		4	**13**
Internal Systems	2					2	3	1	5	**13**
Assigning Responsibility			1	2	6	2	1		1	**13**
Branding				2	2	2	2	1	3	**12**
Terms and Conditions		1			4		2			**7**
Selection (of technologies)	4			1			1			**6**
Identity	1				1		1	2		**5**
Registering/Access	1	1		1			1			**4**
Accessibility	1			1				1		**3**
Support/Maintenance	1									**1**
other	4		4	6	16	14	4	3	20	**71**
Malicious Acts			13	1	5	3	3	2		**27**
Total	**26**	**3**	**80**	**54**	**121**	**90**	**75**	**40**	**68**	**557**

The texts therefore suggest that what distinguishes institutional from non-institutional technologies, is not whether the technology is used or promoted by members of the institution, but whether the technology is owned, provided, approved or managed in some way, possibly by a central department. This is consistent with Weller's (2010) concept of 'centralised' and 'decentralised' technologies.

What responsibilities are assigned to teaching staff when non-institutional technologies are utilised for educational purposes?

Two artefacts explicitly stated that the policy/guidance applied to academic staff, and two explicitly stated that they applied to all staff. The remaining five artefacts did not explicitly state the intended audience, but indicated that they applied to all staff through use of the term 'staff' in the artefact title or throughout the text.

Over 500 rules were identified in the artefacts analysed, many of which related directly and explicitly to issues of safety, security, privacy and data protection (see Table 6). Rules and responsibilities concerning these risks were diverse and in some cases complex. For example:

- to conduct risk assessments (to include assessment of copyright and data protection risks, compliance with institutional policies and potential impact on institutional reputation),
- to identify and assess privacy implications,
- to ensure that online accounts are adequately secured (e.g. through appropriate password selection and maintenance),
- to determine whether users will receive spam mail,
- to set up and manage accounts and data,
- to monitor and intervene in circumstances of inappropriate behaviour or activity and
- to inform students of the risks and seek consent.

This raises a number of questions concerning the role and duties of teaching staff, and the digital literacies that would be necessary to fulfil these requirements. However, it is important to note that a number of artefacts make reference to institutional sources of support, such as IT and learning technology departments, legal services and library teams.

Despite the quantity and breadth of the rules identified, there were some notable omissions. Three artefacts did not contain any rule or reference to security risks, and two artefacts only made one statement relating to security (specifically concerning individual responsibilities to ensure accounts are not compromised, and to change passwords when members leave the institution). Encrypting data is widely recognised as an essential requirement for a minimal level of security (Alim *et al*. 2017). Nevertheless, reviews of educational technologies have found insufficient encryption, which can put devices and data at significant risk (Kelly *et al*. 2018a). Despite these reports, no artefact contained any rule or reference to data encryption.

A previous study which explored how students perceive requests to use personal devices for classroom learning (Author 2019) found that some participants assumed or expected that learning technologies would have been checked for malware. However, only one artefact (A3, produced by an IT department) made any reference to malware detection and prevention. Furthermore, ethical considerations discussed in the literature (such as the use of student data or content by third parties for commercial gain) were absent within the artefacts.

The degrees of obligation required were suggested by the lexical choices and use of modulation within the artefacts. The term 'degrees of obligation' refers to the '…degrees of obligation to act' (Martin 1992, p. 369), and can indicate the level of authority present within the text. For example, high-level modal verbs, such as 'must', signify a necessity to act and establish a high level of authority, whereas low-level modal verbs, such as 'could', approve or recommend certain behaviours or actions. Most artefacts expressed a median level of authority, but two (A7 and A8, produced by the same institution) opted for a high level of authority, suggesting that a greater degree of compliance is required.

Artefacts A1, A4, A6, A7 and A9 contained question-requests (see Figure 3), that is, demands which are interrogative in their grammatical mood (Fairclough 2003), such as:

- Is the tool suitable for the intended audience, or does it broaden the audience beyond what is appropriate?
- How will the service provider capture, retain and process users' data?
- Could the institutional VLE or other University provided services fulfil the requirements?
- Does the tool comply with accessibility standards?

This approach may be used to persuade rather than dictate responsibilities, and may therefore be considered more collegial in nature (as found in an analysis of social media policies conducted by McNeill 2012). However, according to Ervin-Tripp (1976, as cited in Flöck 2016), question-requests enable the possibility of non-compliance. Furthermore, there is no indication of what would be appropriate answers to these questions. Therefore, if statements are advisory rather than mandatory, could non-institutional technologies be used without the appropriate quality assurance processes or safeguards being in place?

In addition, no artefact clarified the procedures to fulfil the requirements concerning security, privacy and data protection. For example, what steps would you take to determine if the service/app complies with the Data Protection Act? What information would be required and how would this be sourced? What if the information was incomplete or unclear? As outlined within the literature review, there are surreptitious ways that apps and services can collect data, thus demonstrating that this would be very challenging to accomplish, particularly by staff with limited technical and legal knowledge in this field.

To what extent do teaching staff have autonomy to use non-institutional technologies?

Forty restrictions were identified which limit how and when non-institutional technologies can be used. These restrictions include prohibiting the use of non-institutional technologies where equivalent features and functions are provided by institutional technologies, prohibiting use for summative assessment and prohibiting staff from requiring students to use non-institutional technologies. However, the artefact did not clearly define a 'requirement' and thus could be open to interpretation. For example, if a lecturer asked students to watch YouTube videos to prepare for a class, would students interpret this to be a requirement, and if so would this be classified as a prohibited activity (assuming that YouTube would be classified as a non-institutional technology)? Artefact A3 also expressly stated that technical procedures were in place to prevent staff from installing software.

A number of commands were identified (n = 33) which required that staff obtain approval or consent from different individuals or groups including marketing and IT services, line managers and students. This included permission to use (A3, A4, A7, A8), create accounts or profiles (A5, A6, A7, A8) or post-information or content (A4, A5, A6, A7, A8). This is consistent with the findings reported in similar studies (McNeill 2012).

Despite the number of commands, restrictions, boundaries and statements establishing monitoring procedures and consequences for non-compliance, the use of external technologies and social media was actively encouraged in five artefacts, and some artefacts stated the benefits of these technologies more so than the risks (see Table 4).

In conclusion, some institutional artefacts support greater levels of staff autonomy than others. Artefacts that were more advisory in tone may support greater autonomy by encouraging rather than enforcing specific actions. Those that presented rules in the format of question-requests could be seen to promote autonomy by enabling the reader to take an active role in determining appropriate technologies and appropriate practices with those technologies. However, question-requests could be perceived by staff as a barrier rather than an enabler of autonomous practice, if they feel that they do not have sufficient knowledge, capabilities or support to ‘answer’ the questions presented.

Some artefacts could serve to constrain autonomy by requiring, limiting or prohibiting particular uses or behaviours (as discussed above). In addition, the breadth and complexity of the rules contained within these artefacts could suppress autonomy, where staff may feel that they do not have the time, capabilities or resources to comply with the rules. In relation to this, there were 16 statements referring to the consequences for non-compliance and 20 statements related to institutional monitoring, which either occur at a technical or human level, to ensure staff adhere to the rules. These statements may serve to reinforce control through fear of repercussions or monitoring, and thus constrain autonomy. However, institutions may consider this control to be necessary in order to protect the institution, its members and its assets, particularly given the challenges and risks posed by non-institutional technologies.

Conclusion

To explore how UK HEIs are addressing the risks of educational technologies identified throughout the literature, the study assessed 100 artefacts produced by 30 UK HEIs. Nine artefacts (obtained from seven HEIs) were then selected for in-depth analysis. Only one artefact was a dedicated guidance document relating to the use of non-institutional technologies for learning. Six artefacts were focussed on social media technologies. However, there are many third-party learning technologies, such as subject-specific apps and software, content production tools and quizzing/polling services which may not be classified as ‘social media’. This raises the question as to whether there are sufficient policies and guidelines in place concerning the diverse range of non-institutional technologies that can, and are being used for teaching, learning and assessment in higher education.

Over 500 rules were analysed, and the study found that a broad range of responsibilities were assigned to staff (including teaching staff) concerning the selection and use of technologies. Whilst the limitations of data analysis are acknowledged (i.e. conducted by a single researcher, external to the institutions), it can be argued that these artefacts are contributing to defining the role of teaching staff in contemporary HEIs. Mishra and Koehler’s TPACK (Technological Pedagogical Content Knowledge) framework (2006) establishes that technological knowledge is a key component of teachers’ knowledge required for effective technology integration in education. This study has also identified institutional expectations concerning teachers’ technological knowledge. Many of these responsibilities and associated duties require sufficient time, specialist technical and/or legal knowledge and digital capabilities.

There is some evidence that existing institutional policies and guidelines are attempting to address some of the risks of educational technologies as reported within the literature. However, statements or standards relating to security risks and protective measures were absent or inadequate within the artefacts assessed. In addition, the procedures to fulfil these requirements were not sufficiently described. For example, staff were assigned responsibilities to ensure compliance with data protection legislation; however, no artefact stated how this should be achieved. Furthermore, many of these requirements could be difficult to fulfil given the surreptitious ways that data can be collected by apps and services, the difficulties in obtaining information about these technologies due to ambiguous and verbose privacy policies (Reidenberg *et al.* 2015) and the technical and legal knowledge required to ascertain compliance. This may suggest that these artefacts are not establishing achievable standards, but may instead serve to transfer the accountability onto individual users (including teaching staff) and limit the liability of the institution.

A number of contradictions were noted within and across artefacts, including those produced by the same institution. According to Tan (2009), differences and contradictions in policies may result in a misalignment between the intended meaning and implementation in practice. However, this study did not explore how these texts are perceived and implemented in practice or whether existing practices relating to the evaluation and selection of learning technologies are sufficient to identify and minimise significant risks. Furthermore, the study did not explore whether these texts are aligned with student expectations concerning risks and safeguards, or whether they sufficiently address issues concerning students' digital rights. These are areas recommended for further research.

In conclusion, the main aim of this study was to explore how institutions are addressing the risks and ethical considerations of non-institutional technologies, when appropriated for educational purposes. Conole (2013) argues that there must be clear policies and guidelines to support effective institutional coordination and individual experimentation with digital technologies. This study highlights significant inadequacies in institutional policies and guidelines, which could result in ineffective practice in the selection and use of these technologies. A potential consequence could be that technologies are being used without appropriate quality assurance processes and safeguards in place (such as data encryption). Additionally, educational use of these technologies could be discouraged or limited due to the complexities of the responsibilities assigned to users, and insufficient clarity within institutional documentation regarding the quality standards, procedures and terminology used.

However, policies, guidelines and other institutional documents are only one way to support the effective and appropriate use of non-institutional technologies. Hall has asserted that academics must '…have a critical or ethical lens through which to critique the nature of the technologies that they use and re-purpose inside the University' (Hall 2013, p. 52). Thus, this problem also needs to be addressed in the development of digital literacies to empower staff and students to make informed decisions about their devices, data and digital profiles.

Competing interests

The author certifies that there are no relationships or involvement with any organisations which could be considered as a conflict of interest.

Acknowledgements

This research was undertaken as part of the PhD in E-research and Technology Enhanced Learning in the Department of Educational Research at Lancaster University.

The author would like to acknowledge the contribution of tutors and peers in supporting the development of this study and its report as an assignment paper. The author would also like to thank the two anonymous reviewers for their valuable comments.

References

Akande, A. O. & Van Belle, J. (2016) 'The use of software as a service by students in higher education institutions: a systematic literature review', *ACM Press*, pp. 1–6. doi: 10.1145/2971603.2971604.

Alim, F., *et al*., (2017) 'Spying on students: school-issued devices and student privacy', *Electronic Frontier Foundation (EFF),* [online] Available at: https://www.eff.org/wp/school-issued-devices-and-student-privacy

Arpaci, I., Kilicer, K. & Bardakci, S. (2015) 'Effects of security and privacy concerns on educational use of cloud services', *Computers in Human Behavior*, vol. 45, pp. 93–98. doi: 10.1016/j.chb.2014.11.075.

Author (2019) 'An investigation of medical students' perception and willingness to use personal digital devices (PDDs) for classroom learning', *Manuscript in Preparation.*

Aymerich-Franch, L. & Fedele, M. (2014) 'Students' privacy concerns on the use of social media in higher education', in *Cutting-Edge Technologies and Social Media Use in Higher Education,* eds V. Benson & S. Morgan, IGI Global, Hershey, PA, pp. 54–75.

Boag-Munroe, G. (2004) 'Wrestling with words and meanings: finding a tool for analysing language in activity theory', *Educational Review*, vol. 56, no. 2, pp. 165–182. doi: 10.1080/0031910410001693254

Bowen, G. A. (2009) 'Document analysis as a qualitative research method', *Qualitative Research Journal*, vol. 9, no. 2, pp. 27–40. doi: 10.3316/QRJ0902027

Brandtzaeg, P. B., Pultier, A. & Moen, G. M. (2018) 'Losing control to data-hungry apps: a mixed-methods approach to mobile app privacy', *Social Science Computer Review*. doi: 10.1177/0894439318777706

Chatzigavriil, A. *et al*., (2014) *2014 Survey of Technology Enhanced Learning: Case Studies*, [online] Available at: http://www.ucisa.ac.uk/groups/dsdg/asg/~/media/7BCB3F2F-F0E141A79A66BC87DDB34A14.ashx

Coffey, A. (2014) 'Analysing documents', in *The SAGE Handbook of Qualitative Data Analysis,* Sage, London, United Kingdom, pp. 367–379, [online] Available at: http://methods.sagepub.com/book/the-sage-handbook-of-qualitative-data-analysis/n25.xml

Common Sense (n.d.) *Standard Privacy Report Questions,* [online] Available at: https://privacy.commonsense.org/resource/standard-privacy-report-questions

Conole, G. (2013) *Designing for Learning in an Open World*, Springer, New York.

Conole, G. & Alevizou, P. (2010) *A Literature Review of the Use of Web 2.0 Tools in Higher Education,* [online] Available at: https://www.heacademy.ac.uk/system/files/conole_alevizou_2010.pdf

Fairclough, N. (1993) *Discourse and Social Change*, Polity Press, Cambridge.

Fairclough, N. (2001) 'Critical discourse analysis as a method in social scientific research', in *Methods of Critical Discourse Analysis,* eds R. Wodak & M. Meyer, Sage, London, pp. 121–138.

Fairclough, N. (2003) *Analysing Discourse: Textual Analysis for Social Research,* Routledge, London.

Farahmand, F., Yadav, A. & Spafford, E. H. (2013) 'Risks and uncertainties in virtual worlds: an educators' perspective', *Journal of Computing in Higher Education*, vol. 25, no. 2, pp. 49–67. doi: 10.1007/s12528-013-9067-5

Flöck, I. (2016). *Requests in American and British English: A Contrastive Multi-Method Analysis,* John Benjamins Publishing Company, Amsterdam.

Gadd, E. & Weedon, R. (2017) 'Copyright ownership of e-learning and teaching materials: policy approaches taken by UK universities', *Education and Information Technologies*. doi: 10.1007/s10639-017-9583-4

Garrett, B. M., MacPhee, M. & Jackson, C. (2013) 'Evaluation of an eportfolio for the assessment of clinical competence in a baccalaureate nursing program', *Nurse Education Today*, vol. 33, no. 10, pp. 1207–1213. doi: 10.1016/j.nedt.2012.06.015

Hall, R. (2013) 'Educational technology and the enclosure of academic labour inside public higher education', *Journal for Critical Education Policy Studies*, vol. 11, no. 3, pp. 52–82. [online] Available at: http://www.jceps.com/archives/437

Halliday, M. A. K. & Matthiessen, C. M. I. M. (2013) *Halliday's Introduction to Functional Grammar,* [online] Available at: https://www.routledge.com/Hallidays-Introduction-to-Functional-Grammar-4th-Edition/Halliday-Matthiessen/p/book/9780203431269

Hardré, P. L. (2016) 'When, how, and why do we trust technology too much?', in *Emotions, Technology, and Behaviors,* eds S. Y. Tettegah & D. L. Espelage, Elsevier, pp. 85–106, [online] Available at: http://linkinghub.elsevier.com/retrieve/pii/B9780128018736000054

Herold, B. (2018) 'How (and why) ed-tech companies are tracking students' feelings', *Education Week*, vol. 37, no. 36, pp. 14–15.

HESA (n.d.) *Student Numbers by HE Provider and Subject of Study,* [online] Available at: https://www.hesa.ac.uk/data-and-analysis/students/whos-in-he

Janks, H. (1997) 'Critical discourse analysis as a research tool', *Discourse: Studies in the Cultural Politics of Education*, vol. 18, no. 3, pp. 329–342. doi: 10.1080/0159630970180302

Kelly, G., *et al.*, (2018a) *2018 State of Edtech Security Survey,* Common Sense, San Francisco, CA, [online] Available at: https://www.commonsense.org/education/articles/2018-state-of-edtech-security-survey

Kelly, G., Graham, J. & Fitzgerald, B. (2018b) *2018 State of Edtech Privacy Report,* Common Sense, San Francisco, CA, [online] Available at: https://www.commonsense.org/education/sites/default/files/tlr-blog/cs-state-of-edtech-privacy-report.pdf

Lenartz, A. J. (2012). 'Establishing guidelines for the use of social media in higher education', in *Misbehavior Online in Higher Education,* eds L. A. Wankel & C. Wankel, Emerald, Bingley, UK, pp. 333–354.

Lindh, M. & Nolin, J. (2016). 'Information we collect: Surveillance and privacy in the implementation of Google apps for education', *European Educational Research Journal*, vol. 15, no. 6, pp. 644–663. doi: 10.1177/1474904116654917

Lorenz, B., Kalde, K. & Kikkas, K. (2012) 'Trust and security issues in cloud-based learning and management', in *Advances in Web-Based Learning – ICWL 2012,* eds E. Popescu *et al.*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 99–108.

Lorenz, B., Sousa, S. & Tomberg, V. (2013) 'Privacy awareness of students and its impact on online learning participation – A case study', in *Open and Social Technologies for Networked Learning,* eds T. Ley *et al.*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 189–192.

Martin, J. R. (1992) 'Macro proposals: meaning by degree', in *Discourse Description: Diverse Linguistic Analyses of a Fund-Raising Text,* eds W. C. Mann & S. Thompson, Benjamins, Amsterdam, pp. 359–396.

McNeill, T. (2012) '"Don't affect the share price": social media policy in higher education as reputation management', *Research in Learning Technology*, vol. 20, no. Suppl. 1, p. 19194. doi: 10.3402/rlt.v20i0.19194

Miller, K. W., Voas, J. & Hurlburt, G. F. (2012) 'BYOD: security and privacy considerations', *IT Professional*, vol. 14, no. 5, pp. 53–55. doi: 10.1109/MITP.2012.93

Mishra, P. & Koehler, M. J. (2006) 'Technological pedagogical content knowledge: a framework for teacher knowledge', *Teachers College Record*, vol. 108, no. 6, pp. 1017–1054. [online] Available at: https://www.learntechlib.org/p/99246/?nl=1

Moher, D., *et al.*, (2009) 'Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement', *PLoS Medicine*, vol. 6, no. 7, p. e1000097. doi: 10.1371/journal.pmed.1000097

Newland, B., Martin, L. & Ramsden, A. (2011). 'eSubmission – UK policies, practice and support', *Proceedings of the European Conference on E-Learning*, 2011, Brighton, UK.

O'Connell, C. (2015) 'Close-up examination of discourses associated with global university rankings: counter-narratives in UK policy context: discourses associated with GURs', *Higher Education Quarterly*, vol. 69, no. 3, pp. 279–294. doi: 10.1111/hequ.12072

Polonetsky, J. & Tene, O. (2014) 'Who is reading whom now: privacy in education from books to MOOCs', *Vanderbilt Journal of Entertainment & Technology Law*, vol. 17, no. 4, pp. 927–990. [online] Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/vanep17&div=31&id=&page=

Pomerantz, J., Hank, C. & Sugimoto, C. R. (2015) 'The state of social media policies in higher education', *PLoS One*, vol. 10, no. 5, p. e0127485. doi: 10.1371/journal.pone.0127485.

Purvis, A., Rodger, H. & Beckingham, S. (2016) 'Engagement or distraction: The use of social media for learning in higher education', *Student Engagement and Experience Journal*, vol. 5, no. 1. doi: 10.7190/seej.v5.i1.104

Raiman, L., Antbring, R. & Mahmood, A. (2017) 'WhatsApp messenger as a tool to supplement medical education for medical students on clinical attachment', *BMC Medical Education*, vol. 17, no. 1. doi: 10.1186/s12909-017-0855-x

Regan, P. M. & Jesse, J. (2018) 'Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking', *Ethics and Information Technology*. pp. 167–179. doi: 10.1007/s10676-018-9492-2

Reidenberg, J. R., *et al.*, (2015) 'Disagreeable privacy policies: mismatches between meaning and users' understanding', *Berkeley Technology Law Journal*, vol. 30, p. 39. [online] Available at: https://www.jstor.org/journal/berktechlawj?refreqid=excelsior%3A58e6bcb3a0072224316cfbddc06200f1

Saarinen, T. (2008) 'Position of text and discourse analysis in higher education policy research', *Studies in Higher Education*, vol. 33, no. 6, pp. 719–728. doi: 10.1080/03075070802457090

Shon, H. & Smith, L. (2011) 'A review of poll everywhere audience response system', *Journal of Technology in Human Services*, vol. 29, no. 3, pp. 236–245. doi: 10.1080/15228835.2011.616475

Tan, K. (2009) 'Variation theory and the different ways of experiencing educational policy', *Educational Research for Policy and Practice*, vol. 8, no. 2, pp. 95–109. doi: 10.1007/s10671-008-9060-3

Voce, J. (2015) 'Reviewing institutional policies for electronic management of assessment', *Higher Education*, vol. 69, no. 6, pp. 915–929. doi: 10.1007/s10734-014-9813-2

Walker, R., *et al.*, (2014) *2014 Survey of Technology Enhanced Learning for Higher Education in the UK,* [online] Available at: http://www.ucisa.ac.uk/~/media/groups/dsdg/Tel%202014%20Final%2018%20August.ashx

Weller, M. (2010) 'The centralisation dilemma in educational IT', *International Journal of Virtual and Personal Learning Environments*, vol. 1, no. 1, pp. 1–9. doi: 10.4018/jvple.2010091701