# INFORMED CONSENT AND PRIVACY IN SCOTLAND’S PUBLIC LIBRARIES

**SUZANNE CONNOR**

**This dissertation was submitted in part fulfilment of requirements for the degree of MSc Information and Library Studies.**

**DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES**

**UNIVERSITY OF STRATHCLYDE**

**AUGUST 2019**

## DECLARATION

This dissertation is submitted in part fulfilment of the requirements for the degree of MSc of the University of Strathclyde.

I declare that this dissertation embodies the results of my own work and that it has been composed by myself.

Following normal academic conventions, I have made due acknowledgement to the work of others.

I declare that I have sought, and received, ethics approval via the Departmental Ethics Committee as appropriate to my research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to provide copies of the dissertation, at cost, to those who may in the future request a copy of the dissertation for private study or research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to place a copy of the dissertation in a publicly available archive.

(please tick) Yes [X] No [ ]

I declare that the word count for this dissertation (excluding title page, declaration, abstract, acknowledgements, table of contents, list of illustrations, references and appendices) is: 21,983

I confirm that I wish this to be assessed as a Type 4 Dissertation

Signature: Suzanne Connor

Date: 13 August 2019

# ABSTRACT

With the rise of libraries offering digital services to patrons, this work explores the approach of libraries to protecting patrons' privacy when accessing these services. The research focuses on assessing the philosophical and legal issues of privacy and informed consent, and how the privacy policies in place in Scottish libraries tackle these issues. In order to do so, Freedom of Information requests were made to the 32 local authorities responsible for operating libraries in Scotland to provide the documentation used to manage privacy and data protection in libraries with a view to assessing the types of policy used and the themes present in these policies.

The aim of the research was to firstly come to a understanding of informed consent, a term which originated in medical negligence law, and how this concept operates with respect to digital services; secondly, to assess the privacy concerns inherent in the use of digital services, particularly in libraries, and why it is important that users understand and consent to the use of their personal information; and thirdly, to evaluate the privacy documentation on offer in Scottish libraries as to how they take on these issues.

Through undertaking this research, it has been discovered that, while libraries in Scotland have gone some way to addressing data protection, privacy, and consent in their policies and documentation, more could be done with these policies to ensure that privacy concerns are addressed and that patrons understand the information being gathered and used by libraries, and that patrons may not be able to properly consent to the use of this information because of the lack of explanation. It was also noted that there were several different types of policy, and that there was an uneven distribution of the different types of policy, both overall, and within particular organisations.

As a result of this research, four recommendations were made: for clearer explanations of data protection and privacy as an ethical concept to be made, for consent to be clearly requested and to not be a binary process, for a more holistic approach to be taken to privacy, and for more policies to specifically address the library environment.

# ACKNOWLEDGMENTS

With thanks to David McMenemy for his guidance and advice on this project, and to all of the staff on the ILS degree, under whom it has been a joy to study this past year.

Thanks to Catherine Connor for her endless support.

Thanks to Craig Brown for his companionship, loyalty, and encouragement.

And thanks to James Connor: no one is actually dead until the ripples they cause in the world die away.

## TABLE OF CONTENTS

## LIST OF TABLES AND FIGURES

### Tables

### Figures

# CHAPTER 1: INTRODUCTION

## 1.1 Research Context

Since the phrase first appeared in 1947 (Maclean, 2004), informed consent has become a term of art in both philosophical theory and law. It is a hydra-like concept; touch on one aspect of the theory and two more will appear. It can thus be difficult to come to a full understanding not only of what it means but how it applies to different areas, morally and legally. While its use originated in the medical sphere, there is a growing body of literature recognising that the concept applies in a variety of areas. Here, the digital domain was the focus.

Across Scotland (SLIC, 2015), libraries have been encouraged to provide an array of digital services to their patrons. Access to the internet is fast becoming a necessity of everyday life and offering free at point-of-access digital services in libraries is one method of combatting the digital divide. However, it has been recognised generally that as services become offered digitally at a fantastic rate, the risk to individuals' privacy increases (Nissenbaum, 2010). As tools such as cookies, location services, and other forms of monitoring proliferate, users of digital services must be aware of these privacy concerns, and their rights in relation to them, as well as the responsibility of any service provider towards them. From a library's point of view, this means that it is vital that these rights and responsibilities are made clear to all patrons in order both to best serve those patrons and to protect the library from legal consequences.

Having a working definition of informed consent is therefore a matter of interest to any organisation which provides digital services to others, such as public libraries. This is particularly necessary as libraries attempt to keep pace with innovations such as the cloud; there becomes a danger of "function creep" (Dekkers, 2016) where the documentation that covered existing services at the time of consenting is no longer sufficient to cover the vastly different level of access to private information these services require. Libraries, like other public bodies, often use privacy policies – documents which detail the organisation's approach to privacy and personal information – as a means of managing patrons' privacy knowledge and expectations. However, doubts have been raised as to the efficacy of these policies (Bashir *et al*, 2014).

## 1.2 Research Questions and Aims

Missing from the current literature are some key pieces of information which may assist libraries in dealing with the modern digital world. Faden and Beauchamp's (1986) definition of informed consent was created in 1986. The world has changed in the ensuing 33 years. The first aim is to build on this work to form a definition for a digital age. Missing too is a study of what privacy concerns exist with relation to digital services in libraries and how informed consent ought to be used in these organisations. Finally, the privacy documentation of Scottish libraries as assessed to appraise whether they are sufficient to allow for users to consent in an informed manner to the digital services they are using. Thus, the following research questions were developed:

*Research Question One: What is informed consent and has the definition changed in the modern digital era?*

The history of the term informed consent was explored in a bid to gain a greater understanding of the development of the concept. Its use was traced from the first instance in 1947, through Faden and Beauchamp's (1986) seminal work, to the present day. The role of informed consent in the access to and provision of digital services was explored. Informed consent was assessed in terms of both the legal and the moral aspects of its use, in order to gain a full understanding of the reasoning and justification behind the theory. In terms of law, the focus was on the UK, or Scotland where the matter is devolved; however, where suitable comparisons from other jurisdictions exist, these were drawn, and the jurisdiction indicated as necessary.

*Research Question Two: what are the inherent privacy concerns in the digital age and how do these arise with respect to library digital services?*

With scandals such as Facebook's involvement with Cambridge Analytica (Cadwalladr and Graham-Harrison, 2018), privacy often remains a concern for library digital services. Privacy has been a concern in society for centuries, considered in texts such as Bentham's work regarding the Panopticon (Semple, 1993) and Mill's (2011) *On Liberty*. However, the variety of avenues by which privacy can be invaded digitally is far greater than in prior times, and new approaches to both understanding and managing privacy have been identified as necessary (Nissenbaum, 2010). Here, privacy was explored through the literature from its origins to its modern-day conception. The specific necessity of privacy in libraries and how the digital services on offer may cause privacy issues was tracked, with particular reference to Scottish libraries. Finally, the general efficacy of privacy policies was considered.

*Research Question Three: How do the privacy policies of Scottish public libraries address privacy, and do they take into account informed consent?*

With the above considered, Freedom of Information (FOI) requests were made to the 32 local authorities or ALEOs responsible for libraries in Scotland in order to gain access to their privacy documentation. These documents were then subjected to both quantitative and qualitative analysis in order to assess the approach to privacy being taken by Scottish libraries and how much attention these give to consent. The quantitative analysis was performed in order to assess the breadth of types of privacy documentation used in Scottish libraries. The qualitative analysis was performed in order to gain an understanding of the approaches within the libraries and the major themes that appear in the documentation, with a view to assessing how these compare with concerns raised in the literature and making recommendations on how these approaches could change and improve in the future.

# CHAPTER 2: INFORMED CONSENT THEN AND NOW

## 2.1 The Beginnings of Informed Consent

An important component of informed consent is the idea of autonomous decision making. An understanding of autonomy is thus important to any process leading to a definition of informed consent. Kant saw autonomy as "a necessary presupposition of all morality" (Hill Jr., 2013). This was rooted in his wider moral theory that one "ought never to conduct" oneself in any way other than that one would wish that one's "maxim become a universal law" (Kant, 2002, p.18). This formulation was, he posited, the central principle by which rational people with autonomy should conduct themselves. Hill Jr. (2013, p.18) identifies three key components of Kant's autonomy. First, he discusses the concept of the "will" (Hill Jr., 2013, p.18) as the idea that individuals can undertake actions which cause changes in the world around them and do so on the basis of a particular reasoning. This can be further broken down into two discrete aspects:

> [*A*] *legislative practical reason*… that prescribes universal rational norms of conduct (laws) and a *power of choice*… by which we adopt our maxims and choose our particular actions. (Hill Jr., 2013, p.18).

That is, a will that exists as overarching governing principles of behaviour, and a will that dictates our individual actions and decisions. The second component is "negatively free will" (Hill Jr., 2013, p.19) – if we are autonomous rational actors, we have the ability to act in ways which run contrary to our personal desires. The final element Hill Jr. identifies (2013, p.19) is *"freedom positively conceived*"; that while we have negative freedom in that we can act against our inclinations, that we are inherently inclined to act in such a way that is in line with the prevailing moral standards in our society. Our actions are autonomous, because we wish to act in this way, even though we may act in the same way even if we did not wish to do so. This concept of autonomy is part of the central premise of informed consent because, per below, consent must be voluntary and autonomous to be truly informed. While Kant's is not the only philosophical model of autonomy, it ties in well with the idea of informed consent, in that it addresses both the individual and the wider context.

The term "informed consent" first occurred in a letter written in 1947, regarding research being proposed by the US Atomic Energy commission (Moreno and Lederer, 1996). The experiments involved human participation in an environment containing radioisotopes; however, conflict existed as to whether informed consent was necessary, as a previous letter implied that it was not. The confusion here added to what has retrospectively been recognised as an "[abuse] of human subjects" (Moreno and Lederer, 1996, p.228); only the eighteenth and final experiment, which took place after the second letter, involved any kind of consent process. This highlights the degree of importance which naming and invoking the concept may involve, given that it led to a change in procedure.

In 1957, the term was first used in a legal context (Maclean, 2004) in the American case of *Salgo* (1957). In *Salgo*, while it was conceded, there may be some justification for not providing a full list of complications or risks to a medical procedure, the judge continued that "in discussing the element of risk a certain amount of discretion must be employed consistent with the full disclosure of facts necessary to an informed consent" (*Salgo*, 1957). This opinion had also been expressed a few months earlier in an article by McCoid (1957), who, while he did not expressly refer to informed consent, stated that there should be a new "single basis" (McCoid, 1957, p.434) for determining liability in medical malpractice suits: that the doctor was not acting in a manner beneficial to the patient, having not appropriately disclosed the risks of a procedure or having not obtained the explicit consent of the patient.

Even at this stage in the term's development, this argument it proved controversial. Some expressed concerns that it would lead to an offence of strict liability, where all that would need to be proved is that the patient was not informed of the resultant risk, regardless of whether the risk was minimal, or whether the doctor thought it appropriate to omit this information for reason of, for example, not alarming the patient (Meisel, 1977). *Salgo* (1957) was criticised by Marcus Plante. He saw the term of informed consent as being "ambiguous" (Plant, 1968, p.671) and Plante argued that the term caused more confusion in medical negligence cases. As there existed no legal definition other than that which had been developed at case law, Plante saw it as leading to decisions in court which were conflicting and not properly based in rational legal argument. Further, he saw McCoid's (1957) argument as expanding on existing law rather than intending to innovate a new category of basis for suit; it is this innovation that he considered the basis of much of the confusion. He blamed the case for conflating the laws of battery and negligence and making it unclear as to which legal area this rule of informed consent was intended to be established. That the decision had subsequently been made to utilise this concept in negligence cases was, to his mind, an error caused by this confusion (Plante, 1968). Plante's concern was that, while there may be sound cases where consent is an issue, that the overreliance on the term informed consent, which had not been satisfactorily defined, its broadening, and its use without giving it a more specific meaning, especially to the layperson, leads to a situation where any lack of disclosure, however potentially beneficial to the patient, could give rise to negligence (Plante, 1978). This in turn, he argued, could lead to, and indeed already had led to, legislative limitations on medical malpractice suits which would narrow access to justice for patients.

## 2.2 Informed Consent in the UK

In 1957, at the same time as *Salgo* introduced the concept of informed consent in the US, *Bolam v. Friern Hospital Management Committee* (1957) confirmed in UK law that consent could be assumed based on the "reasonable doctor" standard; that is, where the doctor had given as much information as any doctor adhering to a reasonable professional standard could be expected to give. This test, compared to the one applied in *Salgo* and subsequently is a more stringent standard for the patient to meet, as it relies on the claimant being able to prove that no other responsible doctor would have acted in that manner.

The case of *Sidaway Appellant v. Board of Governors of the Bethlem Royal Hospital (and Others)* (1985) appeared in the House of Lords, then the highest court of appeal in the UK. In that case, a patient underwent a procedure which had a 1% chance of causing paraplegia. This risk was not disclosed to her and the patient developed paraplegia. While the decision was made in line with the test set out in *Bolam* (1957), Lord Scarman delivered a dissenting judgment, in which he opined that there was "no reason why a rule of informed consent should not be recognised and developed by our courts" (*Sidaway*, 1985), and the *Bolam* (1957) principle "[did] not cover the situation" as applying it resulted in a patient being unable to exercise their autonomy over their own care, and that factors other than medical probability would have influence over the patient. Maclean (2004) cites this as the first introduction of the concept of informed consent in English law. While there is subsequent evidence of first instance cases which followed the dissenting judgment in *Sidaway* (1985), Maclean (2004) found that there were equal numbers who affirmed the verdict, and as such the doctrine of informed consent was yet to be adopted in England and Wales.

In Scotland, the above cases were affirmed in *Moyes v. Lothian Health Board* (1990). However, the Scots treatment of medical negligence differs from the general principle in the Scots law of delict, which deals with civil wrongs against the person. While the maxim adopted at Scots law, is that of *volente non fit injuria* (to one consenting, no wrong can be done), the onus there is placed on the defender to prove that they informed the pursuer of the risk inherent in whatever course of action was undertaken (*Titchener v. British Railways Board*, 1983). As such, were informed consent to be utilised in areas other than the medical sphere, it is by no means certain that, at Scots law, the onus would be on the pursuer to prove that they were not appropriately informed, but the reverse.

Informed consent also appeared in other areas during this period. Implementing EU Data Protection Directive's (The European Parliament and Council of the European Union, 1995) provisions, the Data Protection Act 1998 required that, absent any of the five other purposes for processing personal data, personal data should be processed only where "the data subject has given his consent" (Data Protection Act 1998, Sch. 2 (1)). While the UK act did not reference *informed* consent, the EU Data Protection Directive (The European Parliament and Council of the European Union, 1995) stated at Article 2(h) that "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes". While no further extrapolation was given on what constitutes informed consent, it is clear that the concept had crossed over into this area of law.

## 2.3 Faden and Beauchamp

In an effort to reconcile the above confusion, Faden and Beauchamp set about compiling their formative text on informed consent, *A History and Theory of Informed Consent* (1986). This aimed to synthesise the legal and ethical aspects raised in the thirty years since the term's first use by "[providing] a satisfactory answer to the question 'What is informed consent?'" (Faden and Beauchamp, 1986, p.vii). While this work again concentrates on the medical and scientific application of informed consent, the principles prove useful in developing an understanding of what may be meant when the term is used; indeed, the authors recognised that, while the law had focused on the scientific sphere, that the concept exists across disciplines (Faden and Beauchamp, 1986, p.3).

The authors argue that informed consent is a concept that derives from what they refer to as "moral principles" which govern the subsequent rules, codes, and laws which utilise the term (Faden and Beauchamp, 1986, p.6). That is, that when the term is used in, for example, a code of practice, it is used because of these principles, whether explicitly or implicitly. The principles that influence informed consent are as follows. "Respect for autonomy" is self-explanatory: informed consent is a moral necessity in order to respect the freedom of choice of the individual. The authors are careful not to synonymise the "autonomous person" and the "autonomous choice" (Faden and Beauchamp, 1986, p.8), stating that persons who lack autonomy may still make autonomous choices; for example, a person who has full capacity may consent to something without fully understanding the conditions of their consent; they are capable of informed consent but did not fulfil that capability.

The principle of beneficence is, perhaps, more grounded in the medical profession. The authors explore the concept via the principles which govern medical practice: to not only do no harm, but, where possible, to actively benefit the patient and do them good (Faden and Beauchamp, 1986, p.10) While these have been traditionally hierarchised, placing doing no harm as the foremost, problems arise with the black and white statement of such. For example, the authors posit that this hierarchy does not anticipate the situation where the harm involved may be "trivial" but the benefit to the patient "substantial" (Faden and Beauchamp, 1986, p.10); if one avoids doing harm at all costs, the potential improvements to the patient's wellbeing may be lost. The authors instead suggest that we should, "strive to create a positive balance of goods over inflicted harms". They further argue that empowering patients by giving them the opportunity to consent in an informed manner contributes to this good, as having a sense of control tends to lead to better outcomes for patients (Faden and Beauchamp, 1986, p.14).

The third principle, justice, is given less weighting. Acknowledging the prominence this has been accorded in previous literature, the authors state that issue of informed consent attribute to justice can often be understood under both the principles of autonomy or beneficence. However, they also recognise that there are some circumstances, such as the use of prisoners as research subjects, which invoke concerns of justice (Faden and Beauchamp, 1986, p.14-15); if the environment of prison is inherently "coercive", is it just to use such a population as a research pool (Faden and Beauchamp, 1986, p.15)? It is clear from the text, however, that the authors consider justice a far lesser concern than the previous two principles.

The authors then use these moral bases to develop a definition of informed consent that centres on the concept of autonomy. Referring back to the distinction between autonomous people and choices, they then expand that there are choices that are "substantially autonomous" (Faden and Beauchamp, 1986, p.235) and choices that are not so. Autonomous people may make choices without consenting in an informed manner and vice-versa. In order for a choice to be autonomous, the choice must be made "intentionally… with understanding… and without controlling influences" (Faden and Beauchamp, 1986, p.238). These conditions are necessary, if not sufficient for an autonomous choice; that is, it may be possible that even by fulfilling these criteria, a choice may still not be autonomous, but that if these criteria are not fulfilled, it *cannot* be autonomous. The authors use a broad definition of intention, stating that even acts which come about as a by-product of another act can be seen as intentional, if the actor has done this deliberately (Faden and Beauchamp, 1986, p.244).

On understanding, the authors initially write that

> [A] person has… total understanding of an action if the person correctly apprehends all the propositions of statements that correctly describe… the

> nature of the action, and… the foreseeable consequences and possible outcomes that might follow as a result of performing and not performing the action (Faden and Beauchamp, 1986, p.251).

However, this poses two problems. It does not account for the circumstance where a person fully understands a situation, as far as they are aware, but there is information not available to them that would change their understanding; the definition is insufficiently demanding, as that person could not be said to truly understand. Complete and full understanding does not and cannot exist with respect to every single action; the definition is thus overly demanding, as this is an impossible standard to meet. Thus, they revise the definition as follows:

> A person has a *full* or *complete* understanding of an action if there is a fully *adequate* apprehension of all the *relevant* propositions or statements (those that contribute in any way to obtaining an appreciation of the situation) that correctly describe… the nature of the action, and… the foreseeable consequences and possible outcomes that might follow as a result of performing and not performing the action (Faden and Beauchamp, 1986, p.252).

However, problems still arise in how to assess this understanding and in determining what adequate really means. Further, there is the problem of how to deal with those who hold false beliefs about what they are consenting to. The authors posit that one solution to this problem is to assess how "justified" the person is in holding this belief, on the basis of the available evidence (Faden and Beauchamp, 1986, p.254).

The third aspect of autonomous choice is that of "noncontrol" (Faden and Beauchamp, 1986, p.256). The two competing aspects of noncontrol are "influence" by some actor trying to advocate for one particular choice, and "resistance", the ability to withstand this persuasion (Faden and Beauchamp, 1986, p.256). This condition is necessary as choices may be made that are intentional, and understood, but that would have been made differently by the chooser if, say, they had not been held at gunpoint. The threat can be objective (such as a gun) or subjective (presenting a chooser with arachnophobia with a spider). The chooser may be coerced (intentionally threatened in a manner which the chooser believes is credible), manipulated (having their perception of the facts altered), or persuaded (appealing to a particular argument based on reason).

With the above considered, the authors go on to posit that two kinds of informed consent exist: "autonomous authorization" (Faden and Beauchamp, 1986, p.277) and "effective authorization" (Faden and Beauchamp, 1986, p.280) The former judges the validity of consent based on the *prima facie* autonomy of the person's actions, evaluated via the framework laid out above. The latter depends on pre-determined rules or policy to evaluate the validity of consent; that is, if an organisation has a set of criteria to evaluate whether consent has taken place deviation from this would constitute a lack of informed consent. They posit that this is not a theoretical concept impossible to implement in practice – but that "such consents can be obtained frequently… even routinely" (Faden and Beauchamp, 1986, p.280).

Faden and Beauchamp provide not only a coherent reasoning for why informed consent is important but also a structure by which to judge whether informed consent has occurred, which is flexible enough to account for different circumstances; it is clear that they intended for much of the framework to be usable outside the medical sphere. However, having been constructed in 1986, this work fails to address many now commonplace concerns on informed consent in the modern era. With the use of the term having branched into areas other than medicine, and the rapid expansion of digital technology, how has the definition and meaning changed within the last thirty years? Additionally, the text is understandably focused on informed consent in the context of the US legal system. Below, the term is assessed in 21st century context and its further development within the UK.

## 2.4 Informed Consent in the 21st Century

One of the first indicators that change was afoot came in *Pearce v. United Bristol Healthcare NHS Trust* (1999). In that case, a woman cited the non-intervention of a doctor as having caused the still birth of her child and argued that had she been properly informed of the significance of the risk, she would have advocated for different treatment. Here, the court decided that if the risk had been as significant as the 10% she was claiming, the doctor's duty to her would have been breached. In this case, the risk was much lower, and he had not breached his duty. This was the first suggestion of a move away from the *Bolam* (1957) test, toward one more focused on patient choice.

In 2015, there was a reversal of the law. The Supreme Court ruled in *Montgomery v. Lanarkshire Health Board* (2015) that Lord Scarman's dissenting judgment in *Sidaway* (1985), was, in fact the correct approach. Lord Walker opined that "[t]he primacy of the principles of human rights over our own bodies and of patient autonomy is now universally accepted" (*Montgomery*, 2015, p.1434) and that the test set out in *Bolam* (1957) was inappropriate and "ceased to reflect the reality and complexity of the way in which healthcare services are provided" (*Montgomery*, 2015, p.1460) in the modern era. This shift evidences a move towards patient autonomy and away from the perhaps more paternalistic view of the doctor-patient relationship previously prevalent in the UK. More generally, in line with Faden and Beauchamp's (1986) conception of informed consent, it emphasises the autonomy of the decision maker. As such, there has been a shift of the UK law in favour of informed consent.

This shift has not only taken place in the medical world. The rise of the internet and the ease with which information can be shared and disseminated has prompted a change in the way legislators approach consent online. Friedman *et al* (2000) stated that "[i]nformed consent provides a critical protection for privacy" (Friedman *et al*, 2000, p.1). According to statistics gathered in the US at that time, 59% of sites that gather personal information did not inform the user that this was the case (FTC, 2000). Friedman *et al* (2000) agreed with Faden and Beauchamp's (1986) previous work, using elements identified by those authors (though ultimately their definition would move beyond these) to relate how informed consent may be conceptualised in a virtual space. These elements were "disclosure" by the website that information transmitted would be used in a certain way, or retained, "comprehension" by the user of what they are transmitting and how it will be used, "voluntariness", in that the user must give up this information of their own free will, "competence" of the user to understand what they are transmitting and "agreement" of the user in a clear manner to this use of their information (Friedman *et al*, 2000). It is recognised in this article that the issue of judging comprehension and competence become far greater when considering a remote exchange of information compared to the in-person exchanges considered by Faden and Beauchamp (1986). Additionally, they posit that with the increase by many organisations in moving opportunities such as job adverts online, the condition of "voluntariness" may become harder to fulfil (Friedman *et al*, 2000).

The necessity for some regulation in the digital sphere was also recognised in both the UK and EU. In 2002, the EU introduced what became commonly known as the "ePrivacy directive" (The European Parliament and Council of the European Union, 2002). This required that users were informed of the use of cookies – text files which record information about a user's visit to a particular site – and give the user an opportunity to refuse the use of these. The "cookie directive" (The European Parliament and Council of the European Union, 2009) updated the previous rules to require websites to obtain informed consent to cookies which track personal data from the user, although it was opined that that this consent could be implied (Ustaran, 2012) and suggested that many types of cookies may not meet the threshold of personal data to require explicit consent. As such, while there was clear lip service to the idea of consent, it has been argued that such consent was "engineered" (Borghi, 2013), in that the user was not truly informed of the parameters of their consent and the risk remained that people would consent simply to gain access rather from genuine understanding.

However, the introduction of the General Data Protection Regulations (GDPR, The European Parliament and Council of the European Union, 2016) both expanded the scope of what constitutes personal data and narrowed the way in which it can be used. GDPR introduced six new principles under which personal data can be processed, including by the consent of the data subject. It specifies that this consent must be "freely given, specific, informed and unambiguous" (The European Parliament and Council of the European Union, 2016, Recital 32) though these are not replicated in the UK Data Protection Act 2018, which enacts these provisions. Further explanation on the meaning of each aspect of this varies. The ICO (n.d. c) provides guidance on what each of these terms mean in practice. "Freely given" is further explained: "when assessing whether consent is freely given, utmost account shall be taken whether… [it] is conditional on consent to the processing of personal data that is not necessary" (The European Parliament and Council of the European Union, 2016, Article 7(4)). Less clear is the guidance on "specific and informed". While the Regulation states that in order to be informed, users should know the identity of the controller and the purposes for the processing of the data (The European Parliament and Council of the European Union, 2016, Recital 42-43), and the ICO (n.d. c) recommend that users also be provided with information on the use to which the data will be put and be able to change their mind about consenting at any time (ICO, n.d. c)  In Recital 32, the Regulation specifies that the consent must be obtained by a "clear affirmative act" by the user (The European Parliament and Council of the European Union, 2016). This moves the goalposts from a situation where consent can be considered valid or informed by a user simply continuing to make use of the site, despite having been "informed" about the presence of, for example, cookies. However, the ability to gain such an informed consent online has proved difficult, as discussed in the following chapter.

## 2.5 Informed Consent: Next Steps

Some commentators have opined that informed consent is a "legal fiction" (Epstein, 2006). However, it is submitted that this is not the case; where there is a power imbalance, which it has been agreed legally there is in both of the above situations, utmost importance must be placed on the consent being given being as fully and thoroughly informed as is possible. This is evident in the shift, both in medical and information law, to a patient- and user-centric policy.

How to tell if a consent is informed? Faden and Beauchamp's 1986 construction remains the standard by which informed consent can most appropriately be interpreted – does a person consent intentionally, do they understand to what they are consenting, and do they do so without undue influence on the part of another? This can then be evaluated in and of itself, or within the terms of a policy that embodies these principles. Friedman *et al* (2000) adopt this process and attempt to update it for the modern age. Both of these theoretical structures will be used in tandem in the ensuing chapters to evaluate whether informed consent is possible under the present conditions in libraries in Scotland.

# CHAPTER 3: PRIVACY IN THE DIGITAL AGE

## 3.1 The Law of Privacy

Post-World-War-II, an unambiguous statement of rights was deemed necessary. The first of these was the UN Declaration of Human Rights (1948), to which the United States and the UK are both signatory, which stated that "no one shall be subjected to arbitrary interference with his privacy." Subsequently, The Council of Europe established the European Convention on Human Rights (Council of Europe, 1950) which enumerates various rights, including, in Article 8, the right to privacy. While Council of Europe legislation is not directly binding on the member states, certain agreements such as the ECHR can be directly enforced by the Council, in this case via the European Court of Human Rights (ECtHR). In the United Kingdom, certain Articles of the ECHR (including Article 8) are enforceable in the courts (s.8, Human Rights Act 1998) against any public authority which acts in contravention of these rights (s.6(1), Human Rights Act 1998).

The Article 8 right to privacy is not, however, unqualified. Part 2 of the provision gives a broad scope for authorities to derogate from the right. Case law has provided some guidance on this. Laws can be considered inherently in contravention of Article 8(1); in *Dudgeon v. United Kingdom* (1981) it was ruled that although there was a law against homosexual conduct among men, this law in itself was an interference with the private rights of individuals. Application of a valid law can also be a contravention; it has been considered a breach of the law for a prisoner's correspondence to be censored where, among other issues, the prisoner desired to complain about the conditions in which he was being kept (*Silver v. United Kingdom*, 1981) as this was not "necessary in a democratic society"; the only correspondence that could be stopped on Article 8 grounds was that which actually violated national law.

At this stage there were also some early rulings on technological interferences with privacy. In *Malone v. United Kingdom* (1984), the ECtHR ruled that where there is no express law on a matter, especially one of such an invasive quality as phone-tapping, the state does not have the right to carry out such actions without these being both explicit in the law and reasonably foreseeable by the individual.

This was subsequently confirmed in *Huvig v. France* (1990) and *Halford v. United Kingdom* (1997). The invasive quality of certain media technology was also highlighted in *R v. Broadcasting Complaints Commission ex parte Granada Television Ltd* (1994); in that case, a family's complaint that their permission should have been sought for the use of archival footage of their dead children was upheld. This case also confirmed that the right should not be interpreted narrowly as only applying to the subject of the footage itself but could reasonably be interpreted as applying to close family members.

The above deals with the right of privacy in the years before the proliferation of digital technology. These laws and principles were formulated without the foreknowledge that methods of privacy invasion would undergo such fundamental changes over a short period of time. Information was initially governed by the Data Protection Act 1984, which was the first piece of UK legislation to address computer usage (Jabbour and Rowe, 1995). The act governed the processing of personal data, which was defined as information about an individual from which they could be identified, either inherently or by reference to some other document. However, the first legislation to fully address the increased privacy concerns occasioned by the proliferation of technology throughout society was the Data Protection Act 1998. The 1998 Act defines personal data as any recorded data which can identify an individual, whether directly or by reference to another record (Data Protection Act 1998, s.1(1)). Eight data protection principles were established regarding how the data should be processed (Data Protection Act 1998, Sch.1) in order for it not to violate the rights of a data subject.

A number of cases, in both the UK courts and the European Court of Justice, highlighted the limitations of this law in dealing with distribution of personal information. Several cases have been decided on the basis of the claimant's ECHR rights rather than on their rights under the 1998 Act. For example, in *Murray v. Express Newspapers* (2008) paparazzi photographs of the claimant's children were not counted as personal information for the purposes of the 1998 Act but were a violation of their Article 8(1) rights. In *Google Spain SL v. Agencia Espanola de Proteccion de Datos* (2014), the law was interpreted more broadly, in such a manner that search engines were shown to be collecting data by aggregating information hosted on third-party website, where that information fell under the definition of personal information. This became the first basis for the right to be forgotten. Subsequently, in *NT1 v. Google LLC* (2018), two parties claimed that under the 1998 they had the "right to be forgotten" with relation to criminal convictions that they possessed. The court ruled that while in both cases the information had previously been made public, that the information in question about one of the claimants was incorrect and not of legitimate interest, and therefore should not be publicised for data protection reasons. The other claim failed.

Another piece of relevant law is what became known as "the cookie directive" (The European Parliament and Council of the European Union, 2009), which introduced a need for website users to give a positive consent to the use of cookies, where these cookies were storing their personal information. However, problems persisted, as identified by Ustaran (2012). Nothing in the legislation as written prevented websites from taking an implied consent rather than an explicit one as sufficient. Moreover, cookies that may still generally be thought of as invasive, but that fell short of "actually" collecting and processing information about individuals, such as analytics or advertising cookies, were not explicitly covered in the directive. In order to clarify the law in these and other situations, the GDPR was introduced.

The GDPR (The European Parliament and Council of the European Union, 2016) was enforced in the UK by the Data Protection Act 2018. The eight data protection principles were replaced by six new principles, with a seventh overarching principle of "accountability" (The European Parliament and Council of the European Union, 2016, Article 5(2)). Changes were also made to the bases on which personal data could be processed, with significant restrictions compared with the 1998 Act; it is clear that where none of the five other specific principles apply, the data controller must have consent in order to process personal data. Further changes were also made. Expansions were made to what constitutes personal data: for instance, where the photos taken in *Murray v. Express Newspapers* (2008) were not considered to be personal data under the 1998 Act, they almost certainly would be under the new provisions, as Article 4(1) states that "'personal data' means any information relating to an identified or identifiable natural person".

The legislation also codified the "right to be forgotten" (The European Parliament and Council of the European Union, 2016, Article 17), expanding this right from that established in both *Google Spain* and *NT1*, and limiting the public interest reasons for which personal information can be published to those which are necessary for public health, for certain archival purposes, and for the effective conduct of legal cases. Finally, reporting of breaches must now be done within 72 hours of discovery (The European Parliament and Council of the European Union, 2016, Article 33) and have a significant increase in potential punishment (The European Parliament and Council of the European Union, 2016, Article 84). Owing to the recency of the law, a body of case law is yet to build. However, companies such as British Airways (BBC, 2019a) and Marriott Hotels (BBC, 2019b) have already received high fines for breaching their obligations to their customers.

## 3.2 Theories of Privacy

The concept of privacy has been developed across several philosophical traditions, although it has not often been explicitly acknowledged, particularly in previous years. One example of such is Jeremy Bentham's conception of the Panopticon. Bentham did not, in fact, touch directly on the right to privacy as an overarching concept. However, his development of the concept of the Panopticon laid the foundation for the idea that privacy is central to our lives as human beings and to our sense of freedom and liberty (Semple, 1993). The basic concept of the Panopticon was as a prison where, while there would only be one guard, the prison would be designed in such a way that the guard would be able to observe the inmates without their knowledge. Therefore, any given inmate could not know for certain whether they were being watched at any given time, and as such, behaviour would improve.

Bentham's theory related specifically to the penal sector. Michel Foucault expanded upon this principle in his 1977 work *Discipline and Punish*, to postulate that the "panoptic principle" (1995, p.331) could and indeed does appear in a wide section of society than simply the penal sector. He posits that, hospitals, schools, and other institutions that are part of daily public life can make use of this concept to control the behaviour of their patients, pupils, or other patrons. Essentially, by denying people privacy through their perception that they may be observed – whether or not this perception is correct – it is possible for institutions such as those mentioned above, to influence and potentially change the behaviour of those with whom they engage.

The implication is that to invade privacy – whether in actuality or causing the belief that this could potentially be the case – can have an effect on the liberty of individuals. Can there be any justification for doing so? In terms of the law, this is clear; Article 8(2) defines when there is justification for limiting the rights of the individual. Philosophically, the argument from harm has been employed both as a rationalisation for the restrictions to the right of privacy and in opposition to such. The harm principle derives from the work of John Stuart Mill. Mill conceptualised the harm principle as a justification for limiting the liberty of others: "the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others" (Mill, 2011, p.23). Thus, limitations on the law must only exist to the extent that they will reduce harm to combat "the disposition of mankind, whether as rulers or as fellow-citizens to impose their own opinions and inclinations as a rule of conduct on others" (Mill, 2011, p.27). What is harm? Mill considers an example and concludes:

> No person ought to be punished simply for being drunk; but a soldier or a policeman should be punished for being drunk on duty. Whenever, in short, there is a definite damage, or a definite risk of damage, either to an individual or to the public, the case is taken out of the province of liberty, and placed in that of morality or law. (Mill, 2011, p.94)

In that case, the drunk-driver can be considered harmful as there is the *definite risk* of damage. However, were he merely a drunk pedestrian, the harm principle could not be employed; despite any opinions an individual or society may have on the immorality of public drunkenness, "the inconvenience is one which society can afford to bear, for the sake of the greater good of human freedom" (Mill, 2011, p.94). This clearly maps on to the right to privacy as formulated in the ECHR and to the conception behind data protection legislation, particularly the GDPR; that privacy should be invaded only insofar as this is necessary to prevent harm in society.

Mill's theory has not been without criticism. Schoeman (1992) asserts that in this, and in other aspects of Mill's theory, Mill relies too heavily on the assertion that individuals are rational actors who make decisions based on reason and logic, where the evidence rather shows that conformity is often the more influential factor (Schoeman, 1992, p.34), although he does not see this as necessarily a negative. Schoeman further considers that privacy can be equally burdensome as it is freeing; for example, the idea of the "private family life" can be used as a tool for subjugating women as easily as it can be liberating to other individuals (Schoeman, 1992, p.14). Indeed, he states that "it is only in certain sorts of contexts that privacy and individuality will emerge as feasible and desirable social categories" (Schoeman, 1992, p.114) because of the potential for the use of privacy against vulnerable and minority populations.

The above theories focus on privacy in a general sense, largely with respect to the government or society as a whole versus the individual. However, the popularisation of the internet throughout has allowed for some of the most invasive and difficult to detect incursions into the private lives of individuals. Nissenbaum in her 2010 work *Privacy in Context* sought to create a cohesive work on privacy for the modern age. She states that:

> Information technology is considered a major threat to privacy because it enables pervasive surveillance, massive databases, and lightning-speed distribution of information across the globe. (Nissenbaum, 2010, p.1)

Nissenbaum sees the problem not as people wishing to completely cease the use of their personal information but that they wish to ensure that it "flows appropriately" (2010, p.2) and to feel as if they have some measure of control over how it is used. It is recognised in the text that not all flows of information are equal; for example, a person may feel differently about their personal medical information being used by a hospital for their own benefit than they may feel about their purchases being tracked by a shop with whom they hold a loyalty card (Nissenbaum, 2010, p.6).

Nissenbaum identifies three functions of technology which may invade privacy: "the capacity to monitor and track… aggregation and analysis… [and] dissemination and publication" (Nissenbaum, 2010, p.20). The first of these is the ability of technology to monitor movements and behaviours of an individual over time. The second is the ability to take this and other information, and to evaluate it for patterns or trends, or for any other purposes. The third is the ability to share personal information with others efficiently and effectively. There are various ways in which this can be done; Nissenbaum cites CCTV, mobile phone signals, cookies, internet adverts, and RFID chips such as those found in student cards and other security passes (Nissenbam, pp.21-35). Later, she also identifies web-based resources such as Google Street View, online public records, and social media, (Nissenbaum, 2010, pp.51-58) the last of which perhaps the most significant due to the way in which participants offer personal information via these media. It should be noted that despite being a relatively recent work, the proliferation of smartphone usage and functions such as always-on location-based services had yet to occur. As such, the considerations to be taken into account almost a decade later are more numerous than Nissenbaum covered in this work. However, the central concerns remain the same; what do organisations know about individuals, and how do they know it?

Nissenbaum states that this is "a messy and complex subject" (2010, p.67) to which she hopes to bring some order. She identifies a conflict between neutral or descriptive conceptions of privacy, such as identified by Gavison – that is, where privacy is defined without reference to it having any inherent value – and a normative conception – which entails defining privacy in terms of its inherent moral and ethical value. Nissenbaum criticises definitions falling under the first conception as too rigid for the modern age (Nissenbaum, 2010, p.71); for example, does a person who posts a photo of themselves on the internet lose privacy? Do they lose privacy if a friend posts a photo, perhaps without express permission? What if the photo is of a personal nature and posted by someone who wishes to harm the individual? These situations have developed their own nuances which would be difficult to handle under a neutral definition. However, a normative conception also has its difficulties. Nissenbaum discusses the situation where a person may simultaneously value their privacy but conduct themselves in a way which puts that privacy at risk, such as posting identifying information about their life and family on social media (Nissenbaum, 2010, p.104). In this situation, attempting to develop a normative concept of what privacy is would differ on whether what an individual says was being evaluated, or what the individual does.

The aim of the above is to show the breadth of privacy problems faced by individuals in the digital age. Indeed, in the period since Nissenbaum's work, these have only increased. Not only is there disparity between the importance attached by individuals to privacy, their perception of their success in protecting their privacy, and the effectiveness of the measures actually taken by individuals to combat intrusions into their privacy (Bashir *et al*, 2014) but even accessing the information that would be needed to make decisions about this can be difficult and in many cases leads to what has become known as privacy fatigue (Choi *et al*, 2017), where individuals are simply so overwhelmed by the volume and complexity of privacy concerns that they become unable to determine their best options.

## 3.3 Privacy and Digital Services in Libraries

IFLA states in its manifesto that public libraries, "are provided on the basis of equality of access for all" and "should not be subject to any form of ideological, political or religious censorship, nor commercial pressures" (IFLA, 1994). Why is privacy such an important concept for libraries, and public libraries in particular? Gorman (2015, p.176) cites the increased surveillance due to events such as the 11 September 2001 terrorist attacks and the proliferation of digital technology and social media as key factors in the decreasing level of privacy faced by individuals in their everyday lives. As libraries increasingly adopt digital solutions – for example, electronic Library Management Systems – processes become automated, which potentially can have an impact on privacy. Gorman (2015, p.185) then states that key to the relationship between patrons and libraries is the sense of trust that patrons place in the library. This is particularly true in public libraries, as the patron-base is not specialised in the way that an academic or special libraries' patron-bases may be; as such, the faith that public library patrons put in libraries does not come from a place of prior knowledge but is simply in the inherent trustworthiness of the library and its staff. In order to maintain this trust, patrons must believe that their privacy is protected within the library, both in the sense that libraries will handle their personal information while having regard to privacy, and that they can use the library facilities without unnecessary intrusion into the activities they undertake. How should libraries facilitate this? Gorman (2015, p.188) gives two suggestions as to how this can be addressed through policy:

- Each library should relate its policy to the needs of its own community and the environment in which it operates.
- Library users have a right to confidentiality and privacy. The rights apply to minors as well as adults. (Gorman, 2015, p.188)

As privacy concerns with respect to technology only continue to grow, these suggestions should be borne in mind in order to ensure that policies meet the standards necessary to protect privacy.

As long as public libraries have existed, there have been concerns expressed about the tension between, among others, privacy and surveillance. In assessing the early perceived role of public libraries in educating the masses in order to prevent various social ills, Black (2005) assesses the Foucauldian concepts discussed above and states that "[u]sers of libraries have always been conscious of a rule-bound surveillance, both administrative and physical." (Black, 2005, p.416). As such, whether this is the case or not, patrons of libraries perceive that surveillance takes place in libraries and that this is part of the "price" for using this service. However, this does not mean that surveillance should be unchecked or without limit; indeed, IFLA states that libraries should "strive to ensure the privacy of their users, and that the resources and services that they use remain confidential" (IFLA, 2014) and later that "[l]ibrary and information services should respect and advance privacy both at the level of practices and as a principle." (IFLA, 2015). CILIP has adopted these guidelines, adding that:

> In an age in which the citizen is expected to transact their personal data with both the state and private enterprise (and in which the state and private sector increasingly exchange personal data between themselves), it is vital that the individual is both aware of and in control of how their personal information is used. (CILIP, n.d.)

Further, they add that librarians have a duty both to ensure that private information about patrons is safeguarded and to support and educate users about privacy in their actions both in the library and otherwise. At a Scottish level, the Scottish Library and Information Council (SLIC) have also highlighted the need for librarians to be aware of privacy concerns in libraries, particularly where these intersect with freedom of information or expression (SLIC, 2015).

What features of a library cause concern with respect to privacy? To begin with, something as simple as recording borrower information, which may seem innocuous, can lead to incursions into that user's privacy (for an example, see *Doe v. Gonzales*, 2005). This has led to a culture among US libraries of not keeping any more information about borrowers than necessary; if the information is never recorded, it cannot be requested, and thus privacy cannot be violated (Thielman, 2016).

The increase in digital services available in library spaces is often regarded as a positive. This is for good reason. Access to technology is now being recognised as a right in the face of both its pervasiveness in society and integration into almost every aspect of daily life. A "well-developed, well-maintained, and affordable ICT infrastructure" is a key component of providing access to information (Britz, 2008, p.1172). Digital library services have become essential in order to allow users to utilise the library to its fullest extent for their information needs. This is particularly key in Scotland; one-fifth of people remain without personal access to the internet (SLIC, 2015) compared to 11% of the population of England (DCMS, 2016).

As such, SLIC have made one of their key strategic aims for the period 2015-2020 "promoting digital inclusion" (SLIC, 2015, p.18). Among its goals are to provide e-book lending, Wi-Fi connections, and to otherwise "[m]aximise the opportunities offered by digital systems and media" (SLIC, 2015, p.18). In their quality indicators for public libraries, included as signifiers are "internet access", "web links", and "range of e-books and audio books" (SLIC, n.d, p.23). These goals are understandable, given the information on how many Scots are otherwise without access to digital services. However, it is clear that these services have issues of privacy. IFLA (2014, p.2) highlight two such services: "cloud-based library systems" and "services on mobile devices" including e-book and audiobook apps, especially where these are provided, as is common, via third-party commercial entities. In reality, based on the above discussions of digital privacy, all digital services offered by a library could be considered to have privacy issues.

Simply allowing patrons to browse on the internet creates various concerns: what information about their browsing should a library store? Should information about who was logged on to the computer be stored? What if the government enquires about their browsing history? Many libraries filter access to the internet, in order to keep patrons from viewing material deemed inappropriate by either the library service or the blocking software (Spacey *et al*, 2014). While this may seem acceptable in terms of blocking illegal materials, or materials that can lead to criminal activity, filtering can also lead to blocking of information about, for example, sexuality (Ormes, n.d.), leading to a situation in which a patron may have to reveal sensitive information about their sexuality in order to gain access to particular materials. By blocking content about topics such as sexuality, health, and other sensitive matters, this is creating a "two-tier" situation where those who can afford a private internet connection can access this information, and those who cannot afford this have far more limited access. This creates an uncomfortable situation for the patron where they may have to discuss a private matter with the librarian in order to explain what they were searching and that it is blocked. Indeed, "[f]or those patrons already anxious about using a computer, having to request access to a particular site risks simply turning them away from the Internet altogether." (Jaeger et al, 2006, p.134). One of the most important attributes of the internet as opposed to traditional reference material is that it affords the user a measure of privacy to explore issues and to self-educate. Considering that many still do not have home broadband connections, having to use public access terminals already affords less privacy than doing so at home, without exacerbating this by involving a librarian. In terms of libraries being open to all on an equal footing, this is a clear problem.

In Scottish libraries, technological innovations are being embraced in a variety of ways. SLIC (2015) have identified several of these in their current strategy. Many libraries, such as those in North Ayrshire, are now allowing patrons to manage their borrowing online. North Ayrshire council also pioneered a project called "Appiness", where parents were encouraged to use educational apps along with their children. To combat issues of space, Fife Cultural Trust established the "Wi-Fife" project which extended Wi-Fi to all libraries under their authority. Many libraries, such as those run by Glasgow Life, offer e-books, audiobooks, magazines, and comics through third-party services such as Overdrive, BorrowBox, and RBDigital (Glasgow Libraries, n.d.) All of these services require users to share their personal information, and most require this to be shared with third parties. Given the above discussion of digital privacy, the potential for this to be an incursion into individuals' personal privacy is clear. However, for the purposes of this research, the question is not whether, in actual fact, these individuals are having their privacy invaded, but rather whether the measures taken by libraries are doing enough to allow users to make decisions with regard to what happens to their personal information. It now must be considered what measures libraries take to do so.

## 3.4 Combatting Privacy Concerns

The most common way for libraries to deal with the issue of privacy, both digital and otherwise, is to provide users with a privacy policy. The idea of this is to give users a written record of what will and will not be done with their information, and what to do in various situations where either patrons or libraries believe that this privacy may have been compromised. These policies may be separate policies specifically geared towards the library's digital services, or they may be rolled-up with the library's acceptable use policy (AUP) that the majority of libraries require users to review and sign as part of becoming a member. IFLA do not provide specific guidance on privacy policies, stating only that "libraries should encourage users to be aware  of the implications and provide guidance in data protection and privacy protection" (IFLA, 2014). Similarly, neither CILIP nor SLIC publicly provide guidance on privacy policies; SLIC do host a privacy toolkit developed by Scottish PEN (Scottish PEN, 2018) but this deals more with practical actions to be taken by librarians in relation to privacy rather than the policy itself.

The idea of privacy and acceptable-use policies is clear. Commercial privacy policies are intended to "inform consumers about business and privacy practices and serve as a basis for decision making for consumers" (Jensen and Potts, 2004). The same could be said of those used in libraries. The policy should inform the patron of the library's approach to privacy and thus give the patron a basis for deciding whether to use the library's services. Research suggests that good privacy policies should help the user feel in control and as if their information is being used in a "fair and responsible" manner (Pollach, 2007, p.103). As they are acting as public bodies, privacy policies in the UK should be compliant with Article 8 of the ECHR. These policies also must be GDPR-compliant, and many libraries have separate GDPR policies as well as their privacy policies.

The issues with privacy policies are well-documented. It has been found that most of the time, when presented with a privacy policy, users will agree without reading the terms of the policy (McDonald and Cranor, 2008). Jensen and Potts (2004) found that two major issues that affect whether a policy will be read or not are its accessibility – that is, how easy the policy is to find and how long it is – and readability – the language used in the policy. Pollach (2007) concurs, also finding that many privacy policies not only obfuscate information but do not contain sufficient information for users to make decisions about their personal information. She states that, in her analysis, "online privacy policies have been drafted with the threat of privacy litigations in mind rather than commitment to fair data handling practices" (Pollach, 2007, p.107) and that the format and appearance of the policy can be just as important as the content and language in encouraging users to read them. Another issue is that of "function creep" – where a privacy (or other) policy is used to obtain consent to one usage of data, followed by the policy being subsequently updated to include further usages, without the knowledge of the user (Dekkers, 2016).

Bashir *et al* (2014) note the same and add that a further problem is the binary nature of such agreements; a user either accepts all of the terms, or none of them, even though they may have been perfectly willing to accept some or even most of the terms. Further, they found that even where users do read the privacy policies, the way that they are written means that users are often unable to understand what the policy is stating; the sample population in this study was a relatively educated one, as the setting was academic, and as such this problem may be even greater among those with less access to education. The problem with this is clear when considered in terms of the fact that not only should a public library be accessible for all, but that it is precisely those who have had limited access to education who are more likely to only have access to digital services via the library. Furthermore, according to Bashir *et al* (2014), most of their respondents had experienced situations where they had felt pressured into accepting terms and conditions online to which they were not fully sure that they wanted to agree. The authors then set out the two elements which they had found lacking in privacy policies and which could be improved in order to facilitate informed consent to privacy policies: comprehension and voluntariness. Comprehension relates to the ability to understand the privacy material offered, the ability to become "informed". The authors suggest improvements may be to offer shorter policies in clearer language, to offer "multi-layered" policies with more complex layers of information preceded by shorter, more basic explanations, and potentially to have stricter legislation directly targeting privacy policies (although it should be noted this was addressing the US legal context). Voluntariness is ensuring that consent is not "engineered", that is, that when people consent to privacy policies, it is not because they feel forced into accepting terms which they do not, in fact, find acceptable. Most people in their sample felt that privacy policies were inadequate in this regard, and it was suggested that allowing people to only consent to certain aspects of the policy, and therefore to only certain parts of their information being used, would be one possible solution to this perceived inadequacy.

## 3.5 Libraries, Privacy, and Informed Consent

From the above, it is clear that this is a complex set of problems for libraries to unpack.  That libraries should provide digital services seems to be a necessity in the digital age, particularly if issues of equality are to be borne in mind. Indeed, there is much to be lauded in libraries attempting to provide access on a scale and of a quality that would not normally be available free at the point-of-access. With benefits such as Universal Credit requiring recipients to apply online (Harris, 2017) it is vital that digital services are normalised throughout the library service. Given the lower uptake of private broadband in Scotland compared to the rest of the UK, this is particularly important here.

However, the provision of digital services must be done in a manner which does not inadvertently end up harming the people that the library aims to help. In the previous chapter, informed consent was discussed and defined with reference to the digital age. The privacy pitfalls of technology – and why these matter – have been laid out, and the potential inadequacies of privacy policies as a tool for dealing with these have been detailed. Informed consent has been recognised – both at the law and in theory – as a key component of assessing the validity of any incursion into privacy. It is essential when using the privacy policy to inform patrons about how their information is being used and what they can expect from the library, as the patron must clearly understand what they are agreeing to in order to not only appropriately safeguard their information but to engender and maintain trust in the organisation.

# CHAPTER 4: METHODOLOGY

## 4.1 Research Objectives

In undertaking this research, the aim is to assess whether public libraries in Scotland are sufficiently addressing the needs of their patrons to provide informed consent to the use of their private information when signing up for to use the digital services on offer. Public libraries were chosen as they represent the most common context in which members of the general population encounter library services and as such must account for the most diverse set of needs in terms of ability to provide informed consent and understand privacy concerns. Scotland was chosen in order both to control the number of local authorities which need to be analysed (COSLA, n.d.) and because libraries in Scotland have a common cultural context. According to SLIC (2015), there are over 600 library and library-adjacent service points in Scotland public library use is higher than in England & Wales, and these libraries are generally staffed by paid workers, including professional library staff, differing from trends in other parts of the UK (Barnett, 2018) This last is important as, when assessing the appropriateness of informed consent to a privacy policy, the assumption that trained staff will be handling these policies will form part of this analysis.

As such, the objectives are:

1. To further the understanding of the meaning of the term "informed consent", especially regarding the use of digital services.
2. To explore how "informed consent" and concerns regarding privacy (especially digital privacy) relate to each other.
3. To understand what the approach in libraries has been to "informed consent" and privacy, especially where use of digital services may conflict with these issues.
4. To analyse the approach of Scottish libraries to informed consent through assessing the documentation they present to users.
5. To assess whether Scottish libraries have made inroads to ensuring informed consent via this documentation.
6. To recommend future improvements to practice in this area.

The first three of these objectives were assessed via the means of reviewing existing literature on the relevant subjects. To analyse the latter three, a survey via the means of FOI requests will be conducted, in order to gain access to both the privacy documentation provided to patrons and any available privacy guidance or policy used to educate staff with regard to explaining these matters to patrons. This approach was chosen as it allows for a critical analysis to be applied to the actual documentation being used by authorities to inform both members and staff of their privacy policies. It also allows for practical recommendations to be provided. Below, the methods used in creating these requests will be detailed.

## 4.2 Surveys

Parker and Rea (2014) identify three types of information generally identified in surveys: "descriptive, behavioural, and attitudinal" (Parker and Rea, 2014, p.6). For the purposes of this research, the information requested in the FOI requests most closely resemble their conception of descriptive information, that is, factual data about the respondent, in this case, the library service, and the policies they do or do not hold. The sample chosen in this case was pre-determined as aforementioned. FOI requests share some commonality with the "web-based" type of survey as identified by Parker and Rea (2014, pp.12-14). The authors identify the advantages of this type of survey as being, among others, "convenience", "rapid data collection", "ample time", and "ease of follow-up"; The requests also inherently reach a "specialized population" (Parker and Rea, 2014, p.12) as there is a predetermined base of local authorities who will be receiving these and because FOI requests can only be made to public authorities (Freedom of Information (Scotland) Act 2002, s.1). Of the three potential disadvantages raised, only "lack of interviewer involvement" could present a potential issue *(*Parker and Rea, 2014, p.13). This will be mitigated by careful survey design and by the potential for follow-up by email and subsequent requests. As to the others, "limited respondent bases" and "self-selection", these are inherently avoided as disadvantages due to the predetermined base being approached and the legal requirement for local authorities to respond.

Parker and Rea then identify eleven stages of conducting survey research (2014, p.28). These will be used to outline the stages of the survey to be conducted, though not all will apply in an exact manner. The first stage, "identifying the focus of the study and method of research" (Parker and Rea, 2014, p.28.) has been completed already in the introduction to this work, as has the next, which is to establish a budget and research timetable. The "information base" (Parker and Rea, 2014, p.28) in the third stage was developed via the literature review. The sampling stages four and five have less prominence because of the nature of the pre-determined sample discussed above. The sixth stage, designing the survey, is essential conducting a FOI request, as the details of what is asked for will be essential to receiving documentation which will be useful to the subsequent textual analysis. The framework used to design these requests is detailed below. Again, because of the particular facets of a FOI request, stages seven, eight, and nine do not apply. Implementation of Stages 9-11 will follow with the sending of the requests, receipt of the documents, and analysis of the information in NVivo, as expanded upon below.

## 4.3 Freedom of Information Requests

The right to request information from a public authority was instituted in the UK by the Freedom of Information Act 2000. While this has some application in Scotland, the subsequent Freedom of Information (Scotland) Act 2002 covers most of the application of this right in the Scottish jurisdiction. Under Section 1(1) of that Act, "[a] person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority." Section 1(3) allows the organisation to refuse to fulfil the request where the request is not specific enough, as long as the applicant for information is informed that this is the case. Therefore, requests must be as specific as possible; however, as an applicant may not have a clear idea as to exactly what information an authority does hold, there is a balancing act to be performed in their creation. There are 32 local authorities in Scotland. These authorities either directly run the libraries within their jurisdiction or have handed over the running of the libraries to a charitable organisation known as an "arms' length external organisation" (ALEO). That the libraries run directly by the local council are public bodies is clear; while there is no definitive authority stating the same for ALEOs, for the purposes of this research it will be assumed that while these bodies are acting in the manner of a public service, they will be required to follow the same guidelines. Per Audit Scotland (2011), the ALEO's work and services should be in keeping with the council's objectives.

It has been suggested that "researchers are yet to fully appreciate the value" (Savage and Hyde, 2014, p.303) of FOI requests in areas other than journalism. These authors continue that freedom of information requests allow for individuals to undertake research at a scale that would previously have involved a larger organisation to conduct. Savage and Hyde (2014) consider that using the FOI request has advantages and disadvantages. First, while they are ideal to obtain concrete descriptive information from public authorities, they are less well adapted to obtain information about the reasoning behind these decisions. However, they further opine that where comparison between public authorities is sought - as it is, in part, in this research – the instrument is very effective. In order to deal with the volume of the responses, the authors suggest the setting up of a database. In this research, this was done by collating the documents in NVivo and using this both as an organisational and comparative tool. Finally, the authors identify ethical problems with the information retrieved from a FOI request; that the documents may, directly or indirectly, identify individuals. In this research, this was circumvented by anonymising all data up to and including the name of the council to which the information pertains.

The ICO provides guidelines for formulating a FOI request, stating that it should be "clear, specific, focused and unthreatening" (ICO, n.d. b). As the ICO can only provide access to recorded information, the exact documentation to be requested must be considered. The request must be in writing and must contain the applicant's full name and contact information. The ICO recommend avoiding requests which are overly broad, or which are not expressed in a sufficiently serious manner and that it may be helpful for the applicant to state their purpose. If the request is broad or time-consuming enough that the cost of fulfilling it would be prohibitive, the authority is entitled to refuse the request or only fulfil it to the extent that is possible within cost and time constraints.

Similarly, Bourke *et al* (2012) provide a set of four guidelines to creating effective requests. Firstly, that these should be planned, secondly that they should be respectful to the authority applied to, that they should be clear, and that, where necessary, to refine the request. The rubric provided by these authors, as well as that by the ICO was thus used as a basic guideline to construct the FOI requests which are more likely to be responded to positively, with relevant information, and in a timely manner. Thus, the documentation requested was as follows:

1. Any privacy policy or documentation with which you provide patrons of public libraries at the time of becoming members the library.
2. Any privacy policy or documentation with which you provide patrons who are already members who subsequently wish to access any digital services on offer in public libraries.
3. Any privacy policy, information, or guidance displayed publicly in libraries under your authority.
4. Any privacy policy, documentation, or guidance with which patron-facing staff are provided in order to assist patrons with understanding or interpreting the user-facing privacy policies.
5. Any documentation or information relating to any available additional user training which covers privacy when using digital services.
6. Any documentation or information relating to any available additional staff training which covers privacy when using digital services.
7. Any data protection policy or guidance with which you provide staff.
8. Any data protection policy or guidance with which you provide patrons.

These questions were constructed to be specific and clear enough to ensure that local organisations enough latitude to ensure that all relevant policies would be returned. The specific types of documentation requested were drawn from the literature assessed in Chapter 3. The aim was to create a uniform instrument of survey which would request the same information from each organisation; while each request was sent individually, the text of that request remained identical, other than changing the greeting to address the correct organisation, in order that the responses would be obtained on the same basis with no variation. A copy of the template FOI request including these categories can be found in Appendix II.

Each organisation has available either an email address or online form set up to receive FOI requests. These were collated, and the requests were sent on the same day. The aim of this was to keep the response date consistent as each organisation had 20 working days in which to respond to the request. The requests were also sent from a University of Strathclyde email address, in order to ensure that the information was sent and received over a secure server.

The data received was uploaded for analysis in NVivo; the organisations then had to be anonymised. A list of the organisations in alphabetical order was imported in Microsoft Excel. Excel then assigned each a random number, and the list was sorted in the order of the random numbers so that the authorities would be in a random order. Each authority was then assigned a code from LA1-LA32. This was done so that the organisation could not be deciphered from the code by simply applying alphabetical order, while still allowing for grouping by individual authority.

Once this information was uploaded, the documents from each organisation were assigned to a Case. NVivo uses Cases to allow, among other functions, multiple sources of information to be assigned to the one group. Each case, in this instance, represented an individual organisation, anonymised as detailed above. This allowed for manipulation of the data both as a whole and with reference to an individual authority. At this stage the data was fully prepared to be analysed by both methods selected.

## 4.4 Quantitative Analysis

Before performing qualitative analysis, a brief quantitative analysis was performed on the information resultant from the FOI requests. Williamson and Bow (2002, p.285) identify four steps in performing quantitative analysis: coding, entry into a data analysis program, analysis, and interpretation. The authors state that coding is the process of identifying categories into which to sort data by means of a numerical code; for example, for a true or false question, a possible coding would be 1 = True and 2 = False. This should remain consistent throughout. At this stage it is essential to ensure that these categories are exhaustive – that they cover all types of response – and that they are mutually exclusive – that there is no crossover between one category and another (Powell, 1997, p.151). The information should then be entered into a database or other tabulation programme, which will be able to generate the appropriate statistical analysis, depending on the type of study. This information is then for the researcher to interpret.

Eight types of material were requested as drawn from the literature. These were the eight categories into which the materials received from the FOI requests were sorted, as well as a ninth for any material which did not meet the requirements of these categories. Each category was assigned a letter. The document was coded in NVivo according to the below set of categories. The analysis performed was on a nominal basis; that is, a binary question of whether a policy in the below category existed, or not. The goal of this quantitative analysis is to understand the factual extent to which each organisation has addressed privacy with relation to digital methods, and the breadth of the measures by which they have done so; that is, how many of the types of these measures each individual council has undertaken.

NVivo allows the user to identify particular themes as "Nodes". A document can be assigned an overall Node based on a category and the text within the document itself can also be assigned thematic Nodes in order to draw relationship between documents. For this quantitative analysis, the aim was to show the relationship between each Case – that is, each organisation – and each of the nine Nodes, or categories of document. This was in order to show the number of ways in which each organisation had chosen to address privacy concerns. Various types of document were returned by each organisation. Any policy not directly developed by the local authority, ALEO, or library was not included, as this research is concerned with what libraries, and, by extension, local authorities and ALEOs are doing to tackle privacy.

Each document was only assigned to one category. However, multiple documents from the same organisation could be assigned to the same category as more than one document may deal with the same topic or be part of the same theme. As part of the FOI request, these categories were communicated to the organisations. Many of these chose in their response to give direction as to which category they viewed the document as fulfilling. These parts of the response were used as guidance when deciding how to categorise documents, especially those which could be considered ambiguous or as fulfilling multiple functions; however, where the document was indicated as fitting into more than one category, the final decision was made on the basis of the title and content of the document itself. The data, once coded, was formed into two matrices, one of which aggregated the total number of documents in each category, and the second of which compared the numbers of types of documents each organisation had provided. These matrices were then extracted into Excel to allow a suitable graph to be produced.

**TABLE 1 – CATEGORIES OF DOCUMENT REQUESTED**

| Category | Type of Document | Description |
|---|---|---|
| 1 | Privacy documentation – new member | Any privacy policy or documentation that a patron is provided with when initially joining the library. |
| 2 | Privacy documentation – existing member | Any privacy policy or documentation that a patron is provided with when they are an existing member but are accessing the digital services for the first time. |
| 3 | Publicly displayed documentation | Any privacy policy of documentation that is displayed in library branches generally. |
| 4 | Staff policy | Any policy provided only to staff to assist with explaining privacy to patrons |
| 5 | User training | Any information relating to additional user training in how privacy interacts with digital services |
| 6 | Staff training | Any information relating to additional staff training in how privacy interacts with digital services |
| 7 | Data Protection - Staff | Any data protection policy or guidance with which you provide staff. |
| 8 | Data Protection - User | Any data protection policy or guidance with which you provide patrons. |
| 9 | Other | Any other information provided relating to privacy |

## 4.5 Qualitative Analysis

Subsequent to the quantitative analysis, an in-depth qualitative analysis was performed. Qualitative analysis can be defined as follows:

> Qualitative analysis of content involves a process designed to condense raw data into categories or themes based on valid inference and interpretation. (Wildemuth, 2016, p.319)

Miles *et al* (2014, p.6) state that it is not necessary to adhere religiously to one style of qualitative analysis, that instead there are a particular set of behaviours or actions common to most kinds of this analysis. They see these as follows: "assigning codes" to the raw materials; "sorting… through these coded materials to identify [similarities]"; "isolating these patterns"; "noting reflections"; "gradually elaborating a small set of assertions"; and "comparing these generalisations with a formalized body of knowledge". These qualities informed the process undertaken when performing the quantitative analysis. Miles *et al*'s (2014, p.6) assertion that one of the strengths of qualitative data is the "*focus on naturally occurring, ordinary events*" and the data's "*richness and holism*" formed the basis of the decision to perform this type of analysis on the FOI responses as it allows for not only the documents provided to be analysed in and of themselves, but the wider context of the documents existence to be considered. An advantage of the approach chosen is that there are fewer ethical concerns than might generally be the case with regard to survey data (Connaway and Radford, 2017, p.217), as the information is produced by an organisation, one which is aware of the reality of freedom of information requests and with no individual participants.

The data was prepared by collating the files in NVivo, as well as anonymising the data. NVivo was chosen as the tool to organise and code the data for the qualitative analysis. Connaway and Radford (2017, p.292) identify several advantages to utilising Computer Assisted Qualitative Data Analysis (CAQDAS) including flexibility in coding, greater ability to link data and other information such as demography, and searchability. Similarly, the volume of information produced by these requests required to be organised digitally in order for it to be handled by one researcher. Although Connaway and Radford (2017, p.293) also note disadvantages, such as cost, learning curve, and errors with the software, this study has aimed to mitigate these; NVivo is provided by the University at no cost to the user; the software has been used in trial periods and training has been undertaken in its use; and continuous saving was used to attempt to control the likelihood of bugs. A worked example of a coded policy can be found at Appendix I.

The type of analysis to be performed was then considered. Two of the methods developed by Hsieh and Shannon (2005) and cited by Wildemuth (2016) were considered: the "conventional" and "directed" modes of "content analysis". The conventional mode is when the researcher derives their codes or themes directly from the material and is useful where there is minimal literature existing on a particular subject. The directed mode, by comparison, is a more structured approach, where the researcher begins with preconceived categories derived from the literature on the subject, and then develops these themes, and adds further themes, by "[immersing] themselves in the data" (Wildemuth, 2016, p.319). The former approach was taken; the results of the FOI requests were received, collated, and coded in NVivo with respect to categories derived from the data.

Themes which were initially considered during this process were: explicit mentions of consent, explicit reference to the right to privacy, explicit mentions of the right to privacy with reference to digital technology, explicit mentions of privacy concerns with relation to specific digital services (for example, library-provided cloud services), and explicit mentions of what patrons should do if they have privacy concerns. However, these were not used as initial categories, but merely concepts initially considered when approaching the data. The structure set out by Miles *et al* (2014, p.6) above, as well as that set out by Wildemuth (2016, pp.320-323) were used complete the analysis by bringing together the results of this analysis for discussion.

For the qualitative analysis, the aim was to deduce, from the content of the documents provided, the major themes and topics dealt with in these documents, with a view to determining which areas have been the focus of privacy and other related policies in use by the surveyed libraries (and by extension local authorities and ALEOs). To do so, the text of the documents was individually analysed in NVivo; this differs from the quantitative coding where the whole document was coded to one Node. Each code could also be assigned multiple times per document in order to assess the prevalence of that theme within the document as well as among all documents. A balance was struck between taking an approach which was in-depth enough to allow for real, meaningful analysis, and an approach which was so in-depth that themes would become overly granular and difficult to compare and contrast.

This coding was done by reading each document provided and identifying themes in the text. Themes were coded as Nodes, and as the analysis continued, major themes and sub-themes appeared. As such, the major themes were coded as "parent" Nodes and sub-themes were coded as "child" Nodes. Each sub-theme was also coded to the parent to ensure that the overall coverage was consistent. This allowed for a hierarchical structure which showed the overall themes of the documents, as well as subjects within those themes. As a grounded analysis, while the analysis could not be completely free of pre-conceived ideas as to the most likely themes given the preceding literature review, the thematic elements were derived from the text itself. The flexibility of undertaking this coding in a digital manner allowed for themes to emerge organically and be rearranged in the hierarchy as necessary.

## 4.6 Limitations of Research and Alternative Methodologies

As with any research, there were limitations to how this study was performed. Limitations that pertained to this project include time. The project was limited to a 12-week timescale in line with the University's time given to complete a Master of Science dissertation. As such, all research had to me planned with relation to this timeline and as such to scale which would fit within this time. This was with particular relevance to the FOI requests, as time had to be allowed for these to be returned. Had more time been available, the research could have been expanded to a larger area – for example, the whole of the UK – or to include more types of information in the FOI request. As such, the limitation of the research to one jurisdiction and one type of enquiry was part of mitigating the time factor.

The information requested from local authorities clearly only represents one perspective on privacy, and as such this sample is a limitation on the research. As part of the study involves interpreting how useful privacy policies are to patrons, it may have been helpful to have the perspective of the staff and patrons who would be utilising; however, due to the time constraints mentioned above, the focus was required to be narrower. This limited perspective was mitigated by referencing a wide range of literature on both informed consent and privacy from several sources.

A final limitation to the research was the restricted amount of literature which already exists on informed consent in a non-medical context, and particularly informed consent in wider society, rather than simply in a research-participant context. As digital services proliferate, it is anticipated that this literature will become more common and it is the aim of this research to contribute to this. In mitigation of this, the literature review was performed with a view to synthesising the existing literature and creating a common context for the situations in which informed consent can and should exist.

Alternative methodologies were explored to perform this research. One potential methodology was the performance of a different form of survey. In this form of survey, a sample of library patrons, staff, or both, would have been provided with a set of questions to garner both their factual experience of privacy and consent in libraries. The advantage of this would have been an opportunity to garner a variety of perspectives, as this was a limitation on this research identified above. However, there may be increased difficulty in obtaining a representative sample, as number of responses may be weighted in favour of patrons of a particular local authority or in favour of one type of respondent. The time taken to receive a suitable number of responses to be able to perform the type of analysis required may hamper the research to be undertaken. The lack of understanding among the wider population of the concept of informed consent may cause results from such a survey to be insufficiently clear for use in this research.

The other methodology considered for this work was a case study on one particular local authority, where the practices in specific branches within that authority would have been observed, and staff and patrons interviewed to gather opinions on the matter of privacy and informed consent. Again, the advantages of this would have been to gather a variety of perspectives on the situation with regard to privacy, digital services, and informed consent. An added advantage to this would have been to allow interaction between the researcher and research participants, which would allow the researcher to interpret the level of understanding and awareness among participants. However, while this would widen the perspective in terms of type of participant involved, the perspective would, in turn, be geographically narrowed. This may be less useful for attempting to discover a more general viewpoint on the current state of these issues in Scotland as local authorities vary wildly in demographic. As such, the decision was taken that it would be more useful to the current research to have a more holistic approach.

## CHAPTER 5: DATA ANALYSIS AND DISCUSSION

### 5.1 Quantitative Analysis and Discussion

Of the 32 local authorities and ALEOs that received FOI requests, 29 responded. A total of 134 documents and web pages were returned. As aforementioned, these were split into categories depending on the type of document. These categories can be seen in Table 1, replicated again below. Figure A shows how many documents were assigned to each category overall. Figure B shows how many of each type of document were provided by each organisation.

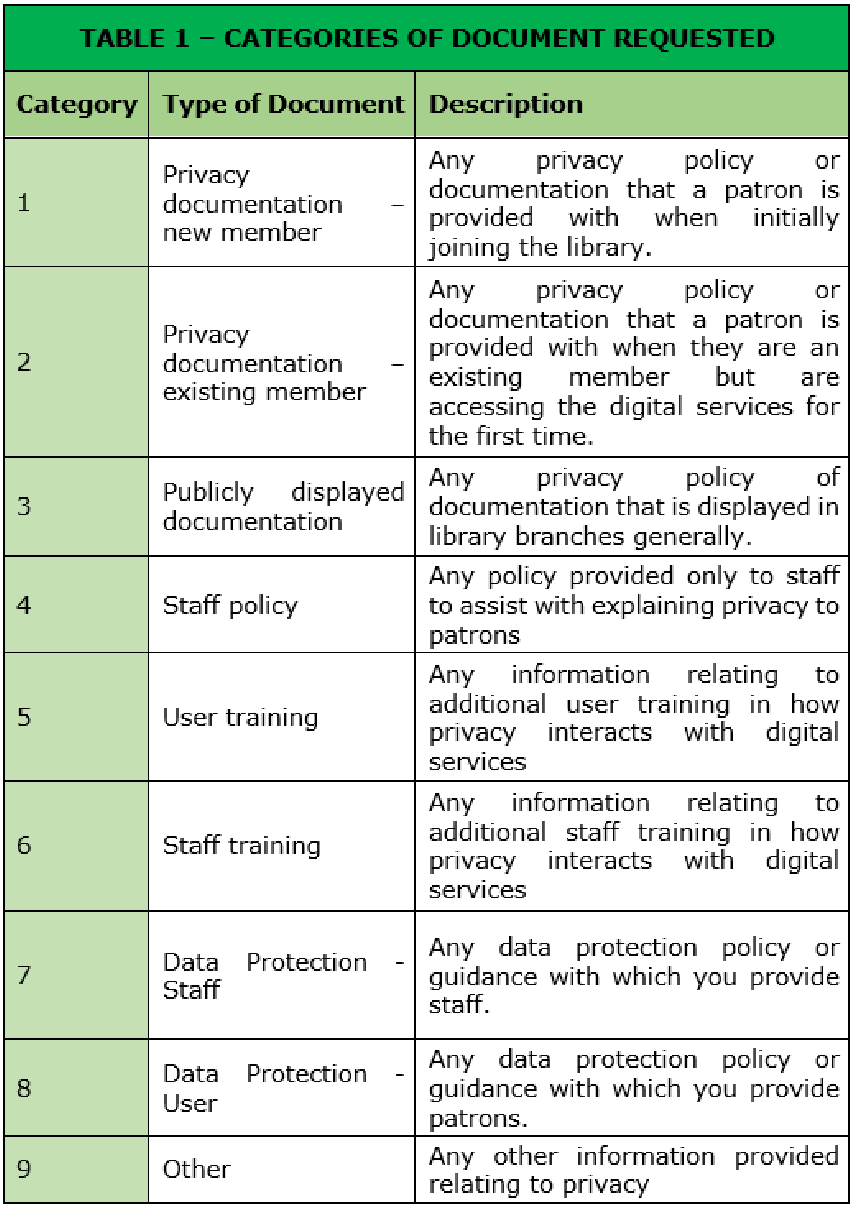


**TABLE 1 – CATEGORIES OF DOCUMENT REQUESTED**

| Category | Type of Document | Description |
|---|---|---|
| 1 | Privacy documentation – new member | Any privacy policy or documentation that a patron is provided with when initially joining the library. |
| 2 | Privacy documentation – existing member | Any privacy policy or documentation that a patron is provided with when they are an existing member but are accessing the digital services for the first time. |
| 3 | Publicly displayed documentation | Any privacy policy of documentation that is displayed in library branches generally. |
| 4 | Staff policy | Any policy provided only to staff to assist with explaining privacy to patrons |
| 5 | User training | Any information relating to additional user training in how privacy interacts with digital services |
| 6 | Staff training | Any information relating to additional staff training in how privacy interacts with digital services |
| 7 | Data Protection - Staff | Any data protection policy or guidance with which you provide staff. |
| 8 | Data Protection - User | Any data protection policy or guidance with which you provide patrons. |
| 9 | Other | Any other information provided relating to privacy |

FIGURE A: NUMBER OF DOCUMENTS IN EACH CATEGORY

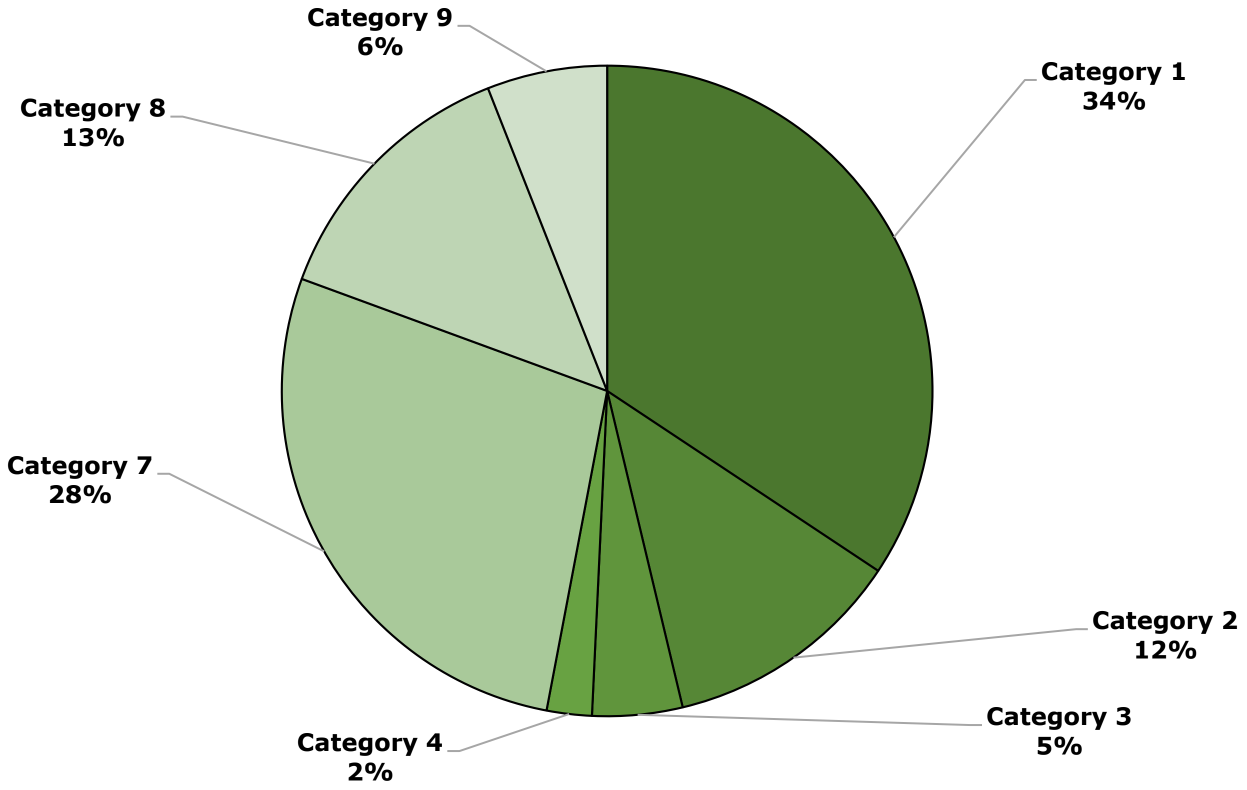
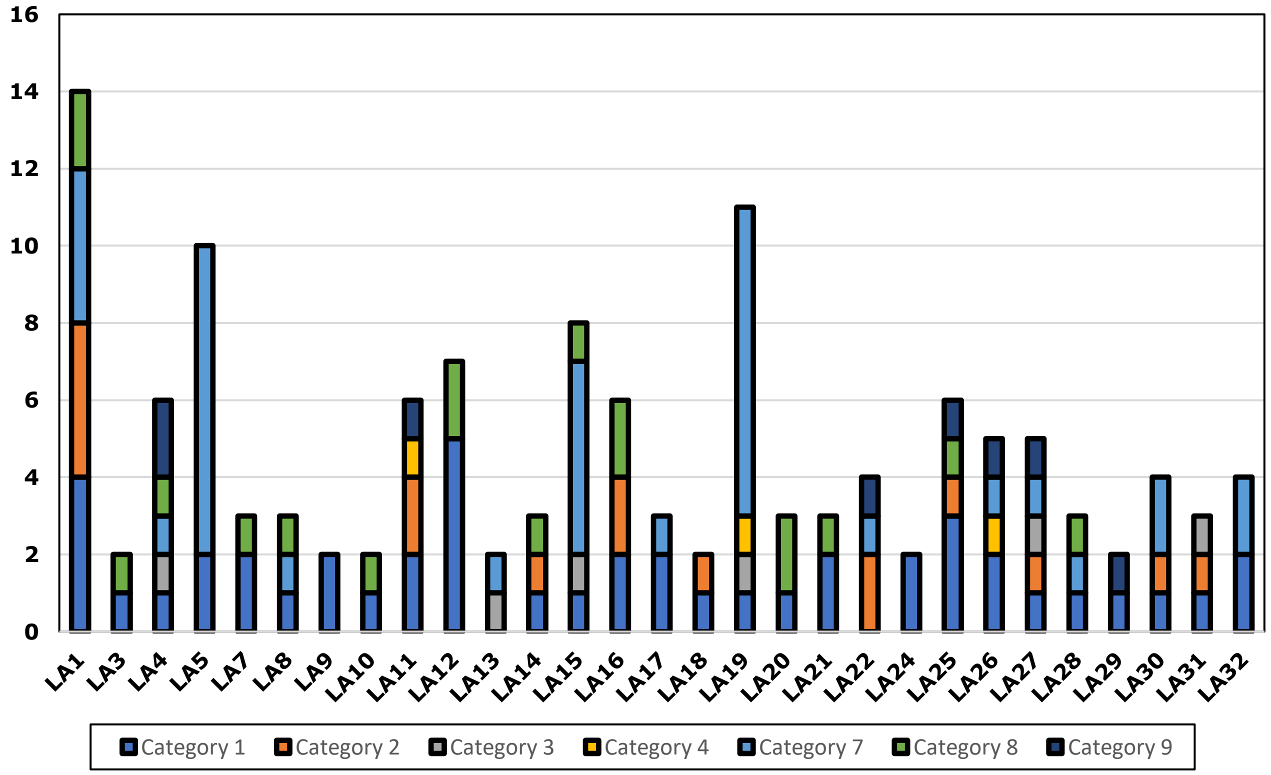


FIGURE B: TYPE OF DOCUMENT BY LOCAL AUTHORITY



As can be seen from Figure A, the most common type of document overall was in Category 1: policies which are presented to patrons when they become members; 46 of these were returned. Fewer than half of that number were policies presented at the time of accessing digital services.  Few of the documents were policies that were primarily displayed publicly; the same was true of policies relating to staff guidance. No policies relating to user or staff training were received. Data protection guidance for both patrons and staff made up another significant portion of the documentation received, though in total still fewer than half of the number of documents which fell into the first category. Of the eight documents that were categorised as "other", six were privacy policies which were available in addition to those presented at time of joining but not specific to digital services, and two were policies for additional services to which the user could opt-in.

In terms of the distribution of policies by local authority in Figure B, the most documents used by one local authority was 14, by LA01; the fewest was two, which seven organisations returned. However, the most categories of document used were by both LA04 and LA27, which had documents in five of the nine areas, despite having returned only six and five documents respectively. Six local authorities had documents in four of the nine areas; only two authorities had documents in only one of the categories. The mean average number of categories represented was 2.83; the mode was 2. The mean average total number of policies was 4.33; the mode was 3. All except two local authority provided Category 1 privacy policies; one that did not provide the policy at time of joining did have a publicly displayed policy and the other at the time of accessing digital services.

It is clear from the above information in Figure A that the provision of privacy documentation is emphasised in particular areas and particular stages of a patron's membership. The most common stage for privacy information to be provided is when the patron becomes a member of the library. As aforementioned, this is regardless of whether the patron wishes to use the digital services of the library or not. A variety of privacy policies were identified as being produced at that stage, as will be discussed further below: common sub-types included dedicated privacy policies (often also containing data protection information) and privacy notices as part of the membership form, which often referred to additional privacy documentation to be accessed at another time. By the time the patron actually wishes to access digital services, fewer than half the number of policies were either in existence or made available. This suggests a lack of reinforcement; rather than being made aware of specific privacy concerns or issues with relation to specific activities within the library, patrons are given a larger quantity of information upfront and may not be given sufficient time or guidance to connect which privacy documentation relates to which type of activity, such as accessing digital services. There is a possibility that this provision of information in such quantities could contribute to a sense of "privacy fatigue" as discussed above, where the patron is unable to cope with the volume of information on offer. This in turn would have a knock-on effect on the ability of the patron to consent in an informed manner, particularly with regard to Friedman's (2000) areas of comprehension, and voluntariness (also reiterated in Bashir *et al*, 2014). The overloading of the patron with information at this stage may cause reduced comprehension, if they do not feel capable of reading a large number of documents for length, time, or other reasons; in turn, this may induce the patron to involuntarily agree to terms that they do not fully understand or wish to comply with, as they feel pressured into doing so in order to access whichever aspect of the service they initially intended.

Fewer still organisations noted that they had separate privacy policies which are publicly displayed, although many noted that the policies they provided at time of joining could be accessed on request or could be accessed online. It is suggested that this may further contribute to a lack of awareness of privacy concerns on the part of the patron and, again, lessen their ability to consent while using digital services, whether these are directly controlled by the library or by a third party. Adding the extra step of having to request the policy is less likely to keep privacy at the forefront of the minds of patrons who are using digital services, rather than making it clearly visible within the library, in order to encourage privacy to be under the constant consideration of patrons.

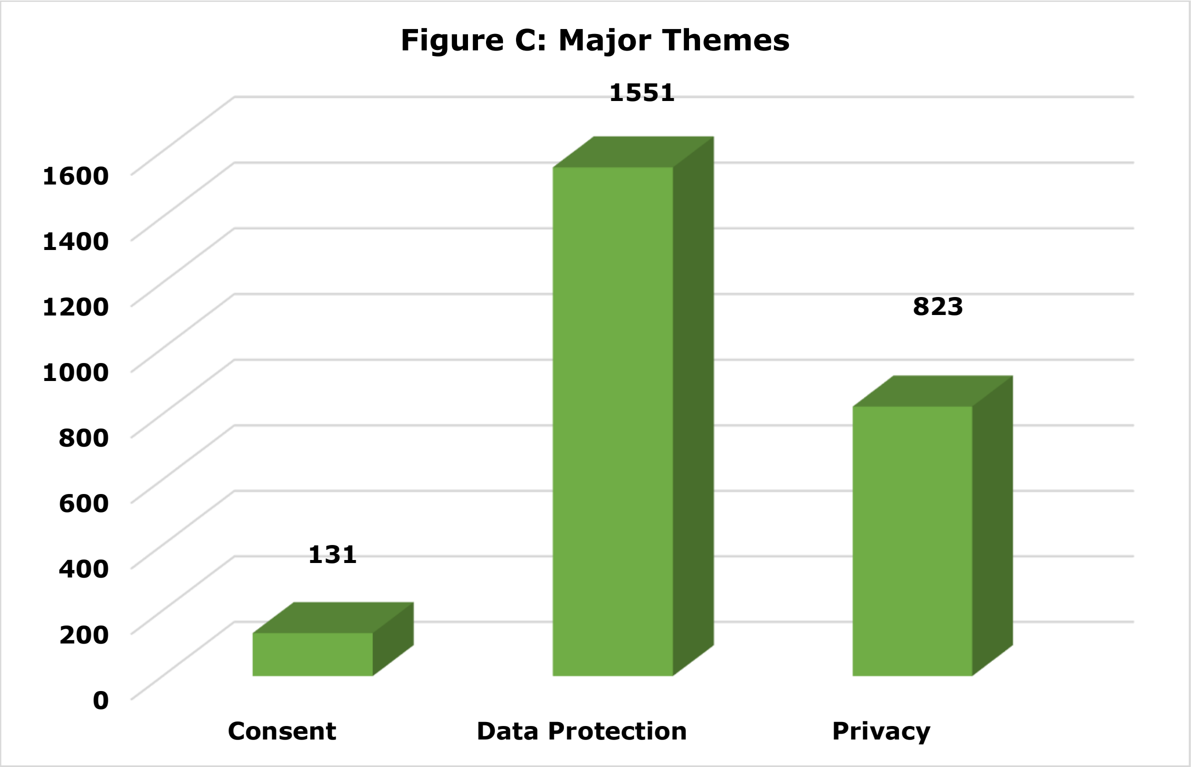
Only three documents were returned under Category 4. Both of these were policies specific to particular situations, and not general staff guidance for dealing with privacy issues. Only one appeared to be particular to patron-facing staff; the other focused on making decisions at the policy level. Taking this in conjunction with the lack of documentation provided in either Categories 5 or 6 (user training and staff training documentation respectively), this suggests that staff may not be sufficiently trained, or have sufficient guidance, to be able to inform patrons about their choices with regard to privacy. For example, having documented guidance for staff to refer to would allow for patrons to be able to discuss more fully privacy at any stage of their service usage. Further, actively training users to assess privacy concerns, especially with relation to digital services, could address issues of privacy fatigue, comprehension, and voluntariness, as a trained professional may be able to contextualise the information provided which the patron is presently left to interpret without necessarily having the ability to do so. It is noted that several organisations stated that their staff were given privacy training but were unable to provide related documentation; as such, this could not be assessed.

Several documents were provided that dealt with data protection, both for staff (Category 7) and patrons (Category 8). While many of the Category 1 documents dealt at least partially with data protection, those in Category 8 were solely concerned with this and were provided in addition to a Category 1 document. Given the recency of the switch to the Data Protection Act 2018, and the new provisions it applies from the GDPR, it follows that many organisations have updated their privacy policies and added separate data protection policies. Patrons should have information about their legal rights available, and staff should be aware of their legal responsibilities in relation to their patrons' information. However, given that these documents are solely focused on legislation, there is a possibility that their content could be seen as overly legalistic, which has been identified as an off-putting aspect of privacy policies (Bashir *et al*, 2014). This will be discussed further below.

Only one organisation covered more than half of the available categories (excluding Category 9: Other). A further four covered four of the eight. As such, the vast majority of organisations addressed privacy in only three or fewer of the areas identified. While this list of categories is not exhaustive, it seems clear from this that few of the organisations surveyed have taken a comprehensive approach to addressing privacy concerns. The GDPR calls for "data protection by design and… by default" (The European Parliament and Council of the European Union, 2016, Recital 78). In other words, data protection (and by extension privacy) should be an inherent part of every organisations approach to their handling of information. Greater coverage of privacy issues, with a variety of approaches, ensures that not only is privacy "baked in" (ICO, n.d. a) to every aspect of dealing with patrons but again that patrons' understanding of these issues will improve, and that libraries can be more comfortable in the likelihood that patrons' use of digital services is done with full knowledge and understanding.

## 5.2 Qualitative Analysis and Discussion

### 5.2.1 Major Themes



The analysis undertaken on the documents was conducted by coding references within the policies based on what they discussed. As the analysis progressed, topics naturally coalesced in to overarching themes, with sub-themes becoming also becoming apparent as the process continued. Three major themes emerged from the qualitative analysis of the documentation. As can be seen from Figure C, the most common topic to be broached was data protection, with 1551 references. The second broad theme was privacy, and the third was consent.

The dominance of data protection is perhaps unsurprising given both the recency and the scale of the changes introduced by the Data Protection Act 2018. Even where policies were designated as a privacy policy or notice (as opposed to a data protection policy), there was a tendency the bulk of the policy to discuss concepts relating to the laws on data protection as opposed to language discussing privacy, or any concerns or practical approaches taken to the same. This approach is potentially problematic. IT puts the focus on the legal dimension of privacy. While it is laudable that organisations such as libraries would wish to give customers a full summary of their legal rights, as well as the organisation's responsibility to protect these, evidence has suggested that lengthy discussions of legal information can be off-putting in privacy documentation as users fail to read them (Bashir *et al*, 2014). The focus on data protection means that while explanation was commonly given of rights and responsibilities, less attention was given to how this information is being gathered, what services have potential privacy concerns, and other practicalities involved in protecting digital privacy. These issues are explored in more depth below.

While consent was a less present theme throughout than either privacy or data protection, where it was referenced, emphasis was placed on it, and as such it was considered a major theme. However, many of the documents assessed did not make any reference to users needing to understand, agree to, or otherwise consent to the terms on offer. Clearly, this gives some cause for concern. Generally, documentation referred to the reason for undertaking the collection of personal information as being for the purposes of performing a "public task" (The European Parliament and Council of the European Union, 2016, Article 6(e)), without any further attempt to clarify understanding or obtain acceptance of these terms. Given the potential problems identified with the emphasis on data protection, ensuring understanding and consent is perhaps particularly essential with regard to these policies. Again, these issues are discussed in more depth below.

### 5.2.2 Data Protection

Figure D: Data Protection Sub-Themes

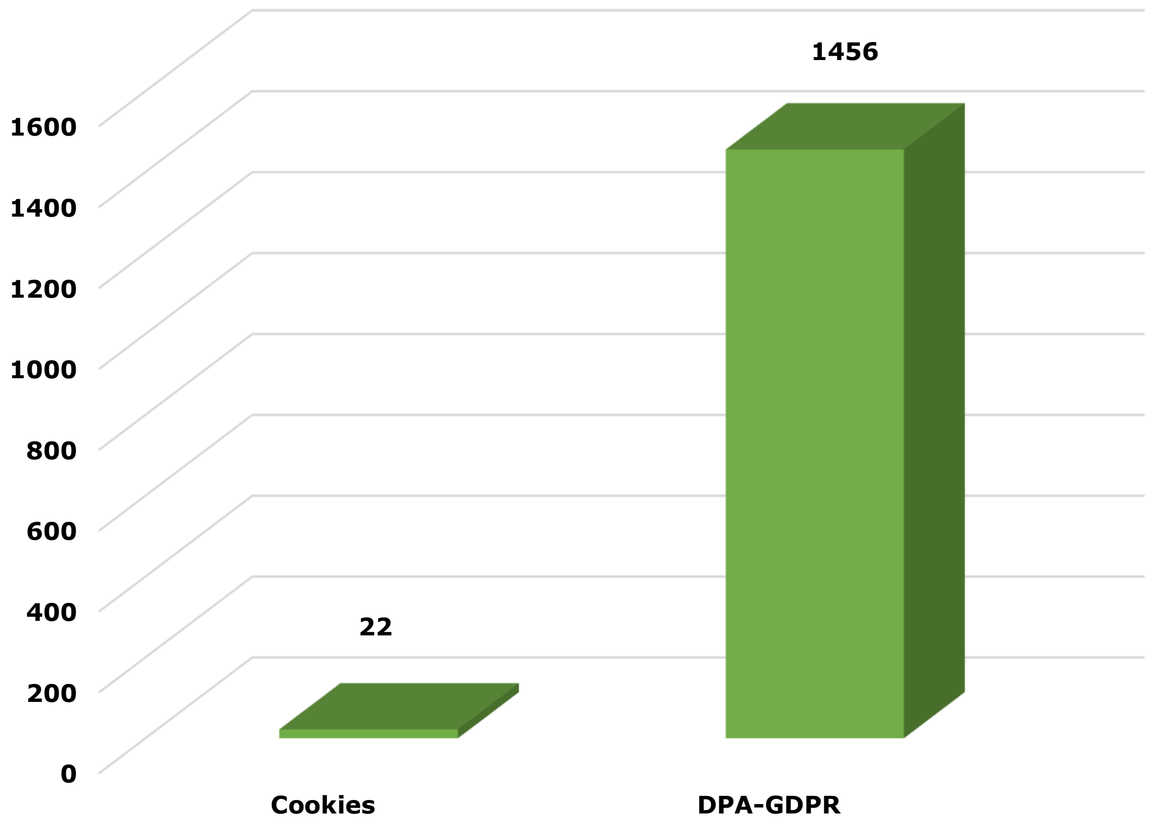
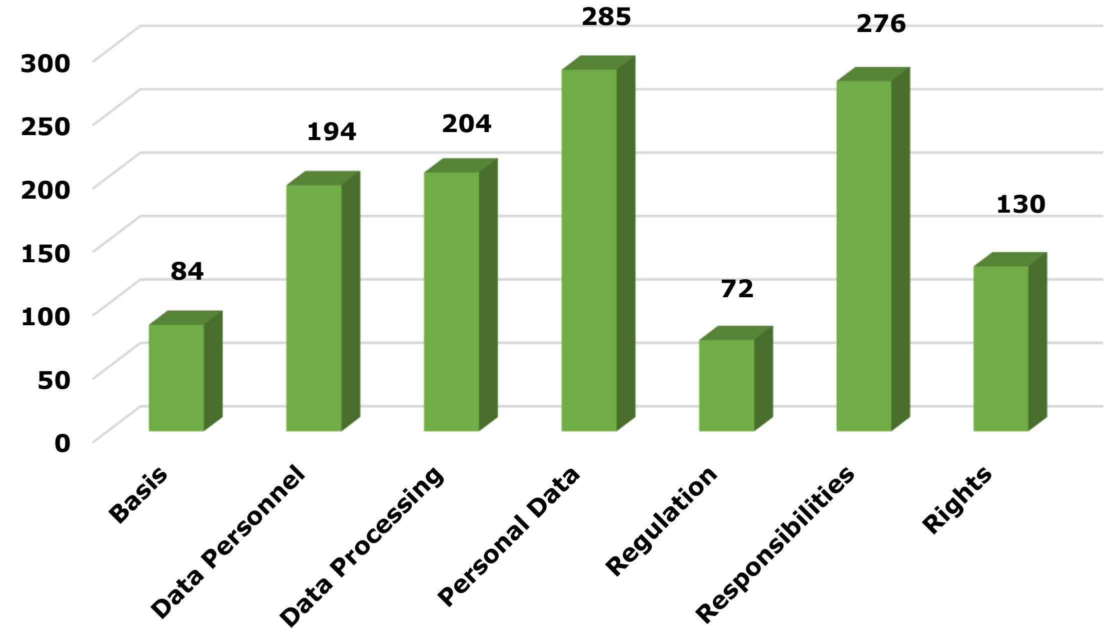


Figure E: Data Protection Act 2018 and GDPR Sub-Themes



Over a total of 134 documents, over 1500 references to data protection were identified, as can be seen in Figure C. These references were split into references to "cookies" and references to the GDPR and Data Protection Act 2018, as well as more general references to data protection. The vast majority of references were to the legislation, as can be seen from the above chart. Only 22 explicit references were counted to the use of cookies or the "cookie directive". Comparatively, there were 1456 references to the GDPR and Data Protection Act 2018. These references were broken down into further sub-themes to analyse which parts of the legislation were the focus. These can be seen in the diagrams above.

The most common theme within the sub-theme of the data protection legislation was "Personal Data". These references ranged from oblique references to personal data such as:

> We will use the data you provide in accordance with GDPR and the Data Protection Act 2018.

To explanations of what personal information is:

> What is Personal Data?
>
> - Data about living, identifiable individuals
> - Any information about an individual, distinguishing them from another
> - Name & address, ID codes, behaviour, choices, health, finances, criminal records

Or direct quotations of the legislation:

> Personal data is defined as 'any information relating to an identified or identifiable natural person' (a data subject).

Each policy tackled the subject of personal data differently – there was no one uniform approach, as shown in the above samples of text. This was the case within the same organisation as well as between organisations, and between staff and user policies; all three of the above pieces of text were sampled from three different policies within LA01, the first being a user policy and the other two staff policies. This difference in the way personal information is explained is despite the basis for these policies being in legislation. From the outset, this could lead to confusion among patrons and staff as to what information they can expect to be protected and what information they can expect to be potentially processed.

Rights and responsibilities were two other themes that appeared throughout the documentation, generally in the format of explaining the patron's rights with relation to their information, and the library's responsibilities towards the same. Both the rights and responsibilities were mostly phrased in legal language, without further expansion, as in this example from LA10:

- The GDPR provides the following rights for individuals:
    - The right to be informed
    - The right of access
    - The right to rectification
    - The right to erasure
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - Rights in relation to automated decision making and profiling.

The above does not actually clarify these rights for patrons. Again, the recourse to legal language decreases the likelihood of patrons reading the policy. The above rights are not defined; the onus is on the patron to interpret their meaning, which they may find is not in line with the actual legal meaning.

Where the legal basis for processing was referred to, the basis was, in each case, specified as "for the performance of a public task". In general, in data protection terms, no further justification was given; some policies offered more general justification for their privacy policies, discussed in section 6.2.3. As no further explanation of this legal basis was generally given, it was not generally clear in which way this specific information would be necessary to complete the function of a library as public entity. While it seems reasonable to expect that libraries may need a name and address to carry out their tasks – as most libraries require members to be resident in the area in which they operate – some of the example documentation required information such as "gender" which may not actually be necessary for operation as a public service. As such, it may be preferable to also include information about the "consent" basis of GDPR (The European Parliament and Council of the European Union, 2016, Article 6(a)).

Data processing was another commonly dealt with theme. The majority of the documentation did not explain what data processing actually entails. Examples of statements about data processing include "[a]ll of the information we collect from you will be processed by staff in the United Kingdom" and "[p]lease note we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law." As such, while processing was frequently mentioned, it was mostly mentioned as part of a broader description of data protection rather than as an individual concept with its own definition. Three policies were clearer about this, one from LA08:

> Processing
>
> Includes obtaining, recording, holding, using, adapting, altering, disclosing, deleting or erasing.

One from LA20:

> [LA20] needs to collect, store, use, share and dispose of personal data in order to deliver services as a local authority. Together, those activities are referred to do as data processing.

And one from LA27:

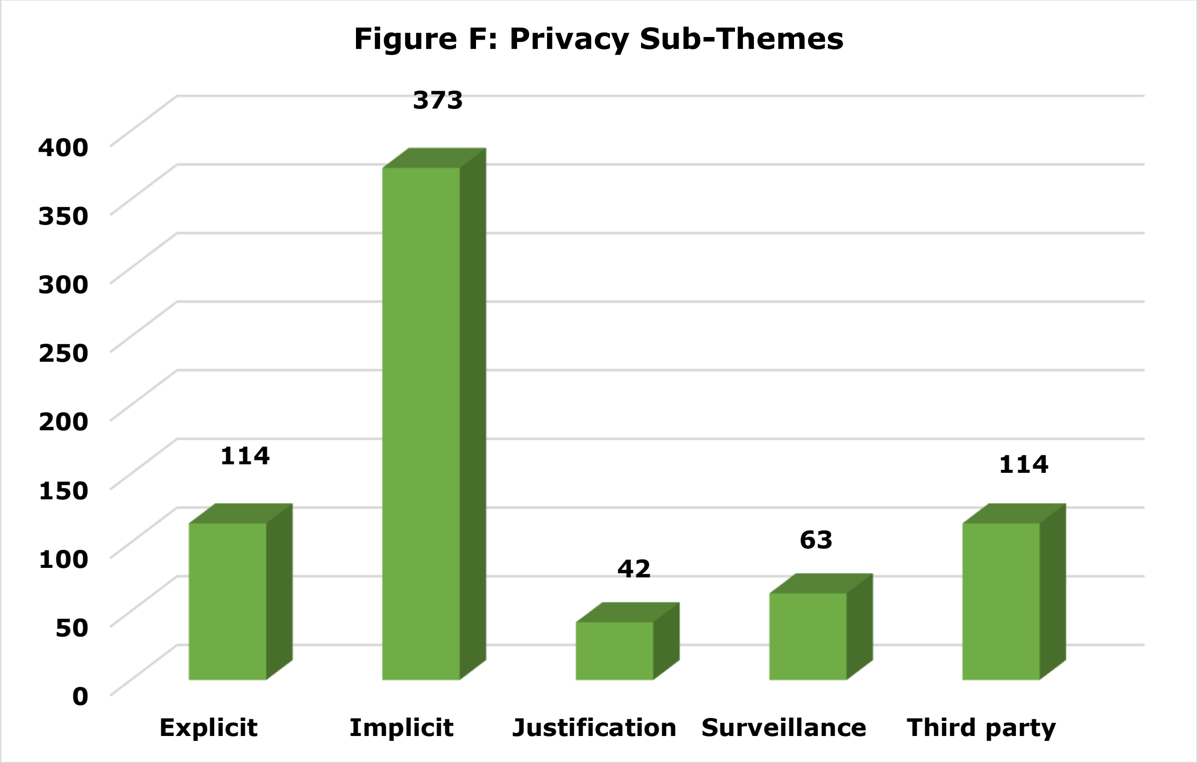
> Processing – Processing is any activity that involves the data. This includes collecting, recording or retrieving the data, or doing work on the data such as organising, adapting, changing, erasing or destroying it.

While these explanations do provide some more clarity, they do not give a full explanation of what the individual authority would be doing with the information. They give a list of potential types of processing without giving a clear account of what processing the specific organisation will be undertaking. Again, this could prove problematic, as, where it occurs in patron-facing policies, it does not allow for patrons to consent to specific types of processing, to have a full understanding of what these types of processing mean, or at least to have some kind of set number of provisions to interpret. Where it occurs in staff-facing policy, while there may be a greater expectation of understanding from their perspective, a lack of clarity in this aspect of the policies impairs the ability of staff to clearly communicate to patrons what they can expect when accessing digital services.

A final pair of themes that arose under data protection legislation were around data personnel and regulation. References coded under those themes include those to potential penalties for breach of the data protection rules, and the personnel to contact in event of a potential breach or (in the patron's case) where dissatisfaction is felt with the way personal data is being handled. Approaches to this varied. Some authorities chose not to define the term data controller, which may cause confusion as to what this actually means. However, the majority were clear both about their role as data controller, the identity of the data protection officer, and the role of the ICO. Where authorities chose to detail the potential penalties, these were largely lifted directly from the GDPR.

The discussion of data protection and the relevant legislation is clearly important to libraries and patrons; in fact, under the most recent law, it is essential. However, the manner in which this is undertaken in the policies analysed leaves room for improvement. Often information or phrases was lifted directly from the legislation with little clarifying discussion in order to assist the patron's understanding. The use of legalistic language does not necessarily allow the layperson to get a sense of what these regulations mean in practical terms and the variation in how concepts were explained, both between different organisations and between policies within the same organisation, could cause confusion. The focus on legality, as opposed to other aspects, may also give the impression that the main focus of these organisations is on their potential legal liability rather than protecting the interests of their patrons. Many of the policies were lengthy, meaning that the effort required to read them, especially in a situation where the patron may want to access services imminently, is more onerous than is perhaps necessary. Certain aspects, particularly around the data personnel and the regulation of data controllers, were generally well signposted and explained. However, the utility of both sets of information when the lack of clarity elsewhere is considered could be seen as questionable.

### 5.2.3 Privacy



Despite many of the documents being referred to as "privacy policies" or "privacy notices", the number of references counted to privacy generally were fewer than those to data protection. While data protection is an important component of any privacy policy – and its inclusion has only become more essential since the changes to the legislation – as discussed in previous chapters it is not the only aspect of privacy that should be discussed within privacy policies and could potentially be seen as giving too heavy a focus to the legal dimension of privacy. As such, a sub-theme that emerged when tracking privacy references were the explicit mentions of privacy (such as explicitly mentioning the word and subsequent explanations) as opposed to references where the implicit theme was privacy, but the word itself was not used.

More than twice the number of implicit mentions were tracked as opposed to implicit. Of those explicit mentions, most were simple the mention of "privacy" in the title. A small number elaborated further; LA25 under the heading of privacy, quoted from the Freedom of Information (Scotland) Act 2002 and ECHR, followed by an explanation:

> The two passages quoted above serve to highlight the conflicting demands which can be placed on the information held by public sector bodies such as [LA25].

While this is more explicit than other explanations, it still takes recourse to legal language and perhaps does not clearly define or explain privacy concerns in the manner appropriate for a layperson. The majority of the references to privacy were implicit. These were any references to themes such as data protection, information sharing, and practical information handling (such as how and where information is stored, both physically and digitally). Having identified the significance of privacy with regard to digital services, it is possible that a lack of clear explanation both of what privacy is – or at least what the organisation perceives as the definition of privacy – and what patrons should pay particular attention to and be concerned about, such as, for example, location tracking services, may cause problems for patrons in understanding and therefore consenting to using these services.

As opposed to the legal basis for processing personal data, references tracked as "justification" were those which were non-legal reasons the various authorities gave for collection of information. Not all authorities provided these types of explanations; many relied only on the legal basis drawn from legislation. Examples of these were they were present included: "[w]e are processing your data for the administration of our Library Services and also for any improvements to this service" from LA26 and:

> To track the location of library stock, administer library membership and other services such as the eBook Service, Home Library Service, Reading Groups and Bookbug Sessions

From LA28. These explanations may assist with informing patrons of the reasons for gathering their personal information and potentially compromising their privacy. However, some clarification could make these explanations even stronger, by connecting the specific type of personal information to the specific activity to be performed and how this information impacts the ability to perform this activity, particularly given the noted problems of comprehension that are pervasive in privacy policies.

Another common sub-theme of privacy that was noted was the theme of surveillance. These references were coded where the policy noted that some type of monitoring is taking place, whether in-person by staff, by cookies which extract information, or in some cases mentions of sharing information with the police. This ties in with the other sub-theme of third-party involvement. This was tracked where there was an explicit mention of the organisation having the ability to share information with any outside party. Again, common examples included law enforcement and other services within the same organisation. However, many policies that mentioned this sharing did not specify which other organisations would be involved. Example measures include:

> Third parties that provide us with support or services may also receive personal, sensitive or payment information, and we require them to maintain security measures similar to ours with respect to such information.

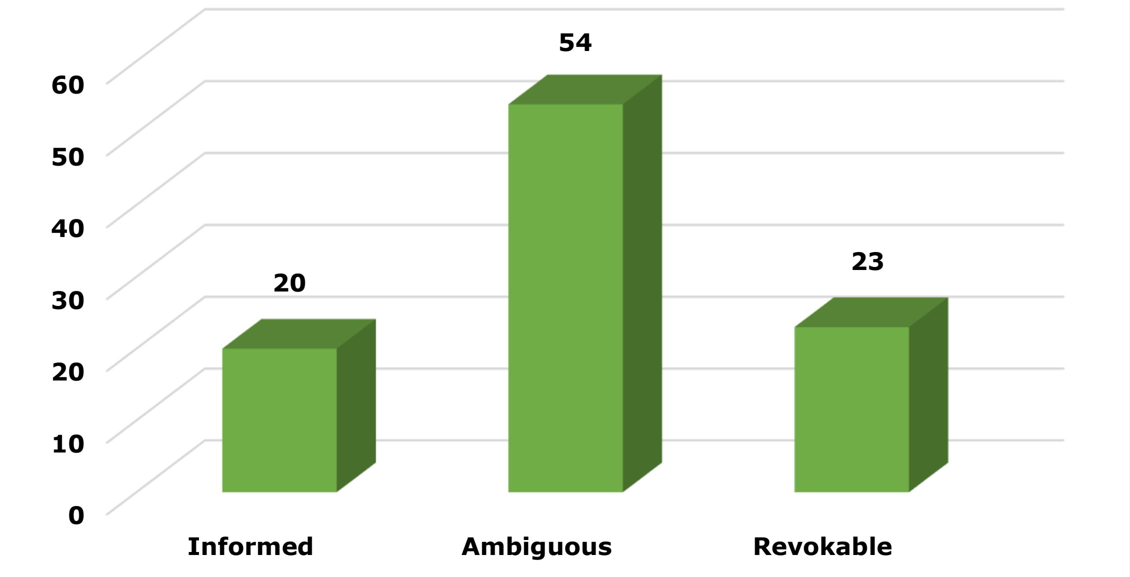
Measures such as these could be considered relatively invasive, given that they do not specify clearly the circumstances necessary for the information to be passed on, and, in the first example, imply an almost panopticon-like approach to handling user information and privacy. This is concerning as these clauses were, in general, not highlighted within the policies and, given the general lack of attention paid to consent, could lead to users agreeing to information sharing and surveillance in a way with which they are not comfortable.

A final sub-theme that developed throughout the policies was the theme of referring to external measures. This was coded where policies referred to other means by which privacy is being managed within the library. In general, this was done by two means: by referring to another privacy policy, or by referring to an acceptable use policy. Often this was done by providing a link to an online copy of a more detailed policy within a document such as a membership form. This could be seen as problematic where the policy requires a patron to go online to view the more detailed version of the policy but to agree to that policy before they can access the internet in the library. As discussed above, for many people, particularly in Scotland, the library is their only method of accessing the internet. Requiring patrons to access a policy online, but only giving them internet access after they agree to that policy, is clearly a situation in which informed consent to sharing of information has not been considered and cannot take place.

As can be seen from the above, most of the policies surveyed have made overtures towards addressing privacy in some form, whether separately from data protection or in tandem. However, the policies in general were not explicit, clear, and detailed on the subject of privacy. While justifications for specific aspects of the policies were present in some of the documentation, these were often not clear or connected to specific practices within the organisations. With the increasing availability of digital services within libraries, it may be more appropriate for more attention to be paid to these matters, and to address the specific potential privacy concerns of particular services, such as cloud storage. Furthermore, highlighting more invasive practices such as information-sharing and requiring specific consent to these could be a more suitable way to approach these practices with respect to ensuring informed consent.

### 5.3.4 Consent

Figure G: Consent Sub-Themes



As aforementioned, the third major theme addressed in the policies was consent. While this was by far the least addressed theme of the three, emphasis was placed on it where it was present. While it may not be expected for staff policies to address consent explicitly, many of the patron-facing policies did not discuss the subject either. Three sub-themes were identified within this area: while it cannot be determined from a document whether any particular consent to be given with respect to it is informed or not, references that seemed closer to allowing for an informed consent were identified as "informed", those which were less clear or in some way problematic were labelled as "ambiguous", and those which made it clear that the consent could be revoked were labelled "revocable".

"Ambiguous" was coded as a reference 54 times. These references were generally coded where the consent asked for involved a policy external to the one actually being signed, where the consent was a check-box consent with minimal guidance and no option for opting in or out of different aspects of the policy and particularly where no reference was made to the patron having to have read or understood terms either included in the document itself or in an external document. Only a few made clear reference to the user having had to read and understand these terms or that the consent must be "freely given". In some cases, it was specified that consent could be revoked where the patron choses to do so; however, several of these cases did not then specify either what would happen with the personal information already or what this would mean for the patron's ability to access services.

While consent is an inherently difficult aspect of these documents to measure without assessing the patron and staff interactions surrounding these documents, there are some ways in which the potential for informed can be assessed. As aforementioned, many of the documents do not mention consent. Of those that do, many do not fully disclose the terms to which the patron must agree, do not mention the need to read and understand the terms that are offered, or present options other than agreement to the document as presented to them. Furthermore, none of the documents presented, either staff or patron facing, mention any assessment as to the competence of the person agreeing. In some cases, the documentation referred to adults having the capacity to agree on behalf of children. In those documents, there was no reference to the child having to understand what was being agreed to on their behalf, and discussions tended to focus on adults ensuring that children abide by the rules laid out, rather than whether the children were capable of understanding these, or had even had the opportunity to see the rules to do so. Under the Friedman *et al* (2000) conception of informed consent, as drawing from Faden and Beauchamp (1986), these approaches in general do not meet the requirements of disclosure, comprehension, voluntariness, competence, or agreement which would be necessary for a consent to truly be informed. In effect, these documents seek to provide "effective authorization" (Faden and Beauchamp, 1986, p.280) – where informed consent can be taken as a given owing to having agreed to the document itself – but do not have the degree of content, either directly related to consent or as described in the sections above, to actually allow this authorisation to form a true informed consent.

# CHAPTER 6: CONCLUSION

## 6.1 Concluding Thoughts

The above work has demonstrated that local authorities and ALEOs have made a strong attempt to address privacy concerns. Most of the documentation assessed clearly addressed the legal obligations surrounding privacy with regard to data protection and did so in a thorough manner. However, beyond the legal dimension, the policies failed to address patrons in a manner which allows for a full understanding of the privacy concerns inherent in digital services.

Informed consent has become a prevalent issue within the digital arena. Having developed from the medical negligence field into a more generalised concept, its characteristics have transformed from their original formulation to suit the various matters in which it has now become central. In terms of the digital sphere, informed consent becomes a concern when digital services are capable of gathering personal information in a high volume and are able to do so without the user of the service knowing, for example, in the form of cookies which can store information. As such, the definition of informed consent and the manner of assessing informed consent must be able to account for the plethora of manners in which digital services are able to obtain this information. As can be seen from the literature assessed in Chapter 2, there have been inroads made into expanding the concept for the digital age, particularly by Friedman *et al* (2000) and Bashir *et al* (2014).

While privacy has been a central concern in libraries for some time, as a result of the changes to both privacy legislation and the types of digital service that can be accessed in libraries, privacy is now more than ever one of the main issues that libraries face. In general, privacy in libraries has been discussed in terms of an ethical obligation. In order for libraries to be able to perform their function to the best of their ability, it is essential that library patrons trust in the library, and an essential aspect of that trust is being able to rely on privacy within the library (Gorman, 2015, p.185). Most libraries use privacy policies to combat privacy concerns; this has borne out in the research undertaken in this work. While this is a common approach, a multitude of problems have been identified with privacy policies as a tool for combatting privacy concerns, such as the length, density of language, and perceived irrelevance of the policy (Bashir *et al*, 2014), and as such this may not be the optimum method for libraries given their increased use of technology.

Having then assessed the privacy documentation provided by 29 of the 32 local authorities and ALEOs in Scotland, positives and negatives were identified in their approaches to the topic of privacy. Many of the policies provided comprehensive information on data protection, including the organisation's approach to such as well as the legal framework behind this. However, given the above identified problems with reliance on legalistic language in privacy policies, it is submitted that the extent of information provided about the data protection legislation, coupled with a general lack of clear explanations of the same in non-legal language, may be off-putting to patrons and contribute to a sense of "privacy fatigue". As identified above, privacy is an ethical obligation of libraries. However, that ethical in itself was often not addressed by these policies; instead, the focus was the legal obligation. Privacy in general was discussed implicitly in the documentation, as a result of data protection rather than an end in itself. If privacy is an essential ethical obligation, it is submitted that it should be more clearly discussed within policies, in particular staff-facing policies in order to instil this value as an inherent part of the library profession.

Where does this leave the idea of informed consent to using digital library services? As identified by Friedman *et al* (2000) there are five elements to informed consent: disclosure, comprehension, voluntariness, competence, and agreement. The policies assessed in Chapter 6 in general did not explicitly address consent. As such, it would be difficult for the level of agreement to be judged. Where consent was mentioned, in general the levels of disclosure varied and could have been improved, particularly in terms of better-quality explanations as discussed above. Most policies also did not mention the necessity of reading and understanding the terms. This does not give sufficient weight to comprehension. While some policies expressly allowed for consent to be revoked, none of the policies allowed for agreement only to specific terms, instead offering an "all or nothing" approach. This has been identified as a problematic situation which can lead to "engineered" consent (Borghi, 2013; Bashir *et al*, 2014) rather than a voluntary one. Assessments as to competence were not made in any of the documentation. In order to improve the approach to privacy in Scottish libraries, these elements should be more thoroughly addressed.

## 6.2 Recommendations

There are several changes that could be made in order to improve patrons' awareness of privacy and ability to consent to the use of digital services. The first of these is to more clearly explain both the provisions of the data protection legislation and to simultaneously provide more comprehensive explanation surrounding the concept of privacy. In order to be able to provide an informed consent, focus must be placed on the concept of "informed". That means that users must be able not only to read and understand these policies, but to be provided with the information that is relevant to them in order to assist with this decision-making. Providing more concise explanations of data protection, which address the parts of the legislation which are most connected with the activities in the library, and which explain how their personal information is being used in connection with these activities. In addition, a clearer explanation of the ethical obligations of the library towards patron surrounding privacy and a discussion of the library's approach to privacy as opposed to the legal obligation of data protection would improve patrons' ability to set their expectations with regard to how much privacy can be expected in the library setting.

A second change would involve putting the focus on consent, offering granulated step-by-step consent, and ensuring that understanding is present throughout. Many of the documents involved did not require consent specifically to be given to that document. While this may be expected with regard to the staff-facing policies, the case was the same throughout many of the patron-facing policies, in particular those which were not referred to at point of becoming a member of the library. If privacy policies are to be used as a tool to informed patrons about their privacy, there should be methods in place to ensure that they have actually been read and understood, especially where the policy is not presented in person. This means drawing attention of the patron to areas which may have particular impact on patron privacy and to emphasise the need for understanding and explaining how staff can assist with this. Patrons should also not have to consent to every use of their data to consent to certain uses of their data. To ask patrons to do so risks engineering consent to situations to which patrons may not actually wish to consent. Instead, consent should be granular and allow for users to decide which services they actually want to use and therefore to provide consent.

A third improvement suggested is to have a holistic approach to privacy. This means covering privacy in a variety of ways and via a variety of methods. Evidence suggests that different people take in information in different ways: visual (images), aural (audio), textual (reading), and kinaesthetic (interactive) (Choolhun, 2012). As such, it may behove libraries to approach both staff and patron privacy information in several different formats, in order for both patrons and staff to be able to be more likely to take in the information and understand it. Libraries also should create policies across the eight categories identified in Table 1 (and potentially other categories). This ensures that no aspect of the approach privacy is weak, no area is left uncovered, and vulnerable to causing a problem. In particular, none of the organisations surveyed provided information about staff or user training with respect to privacy (though some did provide information with respect to data protection training for staff only). Providing training or similar opportunities for both staff and patrons may enable both to have a deeper understanding of privacy concerns.

A final suggestion is that more of the policies should be specific to libraries. Many of the policies provided were organisation-wide policies that applied to all aspects of the running of that organisation. However, as explored in Chapter 3.3, libraries have specific privacy concerns that may not apply across other parts of these organisations. For example, other services may not act as direct providers of digital services. Other services also may have a particular user group; public libraries have to serve a diverse population which have needs beyond those addressed in more general policies. Providing policies which address situations which may only arise in libraries ensures that these needs will be met.

## 6.3 Next Research Steps

Proposals for the next steps in this research will now be suggested. It is suggested that the body of literature on informed consent needs to be expanded. While many texts exist on the subject, the changes that have happened over the last ten, or even five years in the digital world as services such as cloud storage and integration of several services over organisations such as Google, Facebook, and Amazon, means that consent to the use of users' information has never been more essential. As such, up-to-date literature which takes account of these types of services and also future developments in the digital world would allow for a better understanding of how to properly ensure informed consent in the digital era.

Another step that could be taken is to undertake research which directly involves the patrons and staff. This could be done at a remove by survey, or by directly engaging with patrons and staff in a particular service for example in a case study. While assessing the privacy policies allows for evaluation of the approaches taken to privacy, engaging directly with the individuals involved would allow for a stronger evaluation of whether informed consent is actually taking place, and the aspects of the practical, day-to-day approaches in libraries that are contributing to or detracting from this.

A final suggestion for a next step is to assess the reality of the services being used in libraries. Not every organisation uses the same service and each may have different aspects which could have an impact on privacy. Assessing these services may allow for expansion to the literature around privacy in libraries, and if done within a specific organisation may allow for practical suggestions to be made as to how the privacy concerns with regard to those services can be addressed.

## REFERENCES

Anderson, J. and Rainie, L. (2014) *The gurus speak*. Available at: https://www.pewinternet.org/2014/03/11/the-gurus-speak/ (Accessed: 18 July 2019).

Audit Scotland (2011) *Arm's-length external organisations (ALEOs): are you getting it right?* Available at: https://www.audit-scotland.gov.uk/docs/local/2011/nr_110616_aleos.pdf (Accessed: 3 July 2019).

Barnett, D. (2018) "Do libraries run by volunteers check out?" *The Guardian*, 25 June 2018. Available at: https://www.theguardian.com/books/2018/jun/25/do-libraries-run-by-volunteers-check-out (Accessed: 1 August 2019).

Bashir *et al* (2014) "Online privacy and informed consent: the dilemma of information asymmetry". *Proceedings of the Association for Information Science and Technology*, Vol.52(1), pp.1-10.

Black (2005) "The library as clinic: a Foucauldian interpretation of British public library attitudes to social and physical disease, ca. 1850-1950". *Libraries and Culture*, 40(3), pp. 419-434.

*Bolam v. Friern Hospital Management Committee* (1957) Weekly Law Reports, 1, pp.582-594.

Borghi, M., Ferretti, F., and Karapapa, S. (2013) "Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK". *International Journal of Law and Information Technology*, 21(2), pp.109-153.

Bourke, G., Worthy, B., and Hazell, R. (2012) *Making freedom of information requests: a guide for academic researchers*. Available at: http://www.lse.ac.uk/intranet/LSEServices/Legal%20Team/FOI/pdf/academicsGuideFOI.pdf (Accessed: 3 July 2019).

British Broadcasting Corporation (BBC) (2019a) *British Airways faces record £183m fine for data breach*". Available at: https://www.bbc.co.uk/news/business-48905907 (Accessed: 9 July 2019).

British Broadcasting Corporation (BBC) (2019b) *UK watchdog plans to fine Marriott £99m*. Available at: https://www.bbc.co.uk/news/technology-48928163 (Accessed: 9 July 2019).

Britz, J.J. (2008) "Making the global information society good: a social justice perspective on the ethical dimensions of the global information society". *Journal of the American Society for Information Science and Technology*, 59 (7), pp. 1171-1183.

Cadwalldr, C. and Graham-Harrison, E. (2018) "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach". *The Guardian*, 17 March 2018. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (Accessed: 9 July 2019).

Chartered Institute of Library and Information Professionals (CILIP) (n.d.) *Protecting the individual's right to privacy*. Available at: https://www.cilip.org.uk/page/ProtectingTheIndividualPrivacy (Accessed: 18 July 2019).

Choi, H., Park, J., and Jung, Y. (2017) "The role of privacy fatigue in online privacy behavior." *Computers in Human Behaviour*, 81, pp.42-51.

Choolhun, N. (2012) "The Only Way is Information Literacy". *Legal Information Management*, 12(1), pp.44-50

Connaway, L.S., and Radford, M.L. (2017) *Research methods in library and information science*. 6th Edition. Santa Barbara: Libraries Unlimited.

Convention of Scottish Local Authorities (COSLA) (n.d.) *Scottish Local Government*. Available at: http://www.cosla.gov.uk/scottish-local-government (Accessed: 1 August 2019).

Council of Europe (1950) *European Convention on Human Rights*. Available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (Accessed: 17 July 2019).

Data Protection Act 1984, c.35. Available at: http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf (Accessed: 1 August 2019).

Data Protection Act 1998, c.29. Available at: http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf (Accessed: 1 August 2019).

Dekkers, D. (2016) *Privacy or security? – 'function creep' kills your privacy*. Available at: https://www.digidentity.eu/en/article/Function-creep-kills-your-privacy/ (Accessed: 18 July 2019).

Department for Digital, Culture, Media & Sport (DCMS) (2016) Libraries deliver: ambition for public libraries in England 2016 to 2021. Available at: https://www.gov.uk/government/publications/libraries-deliver-ambition-for-public-libraries-in-england-2016-to-2021/libraries-deliver-ambition-for-public-libraries-in-england-2016-to-2021 (Accessed: 18 July 2019).

*Doe v. Gonzales* (2005) Federal Supplement, Second Series, 386, pp.66-83.

*Dudgeon v. United Kingdom* (1981) European Human Rights Reports, 3, pp.40-63.

Epstein, M. (2006) "Why effective consent presupposes autonomous authorisation: a counterorthodox argument". *Journal of Medical Ethics*, 32(6), pp.342-345.

The European Parliament and Council of the European Union (1995) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". *Official Journal of the European Communities,* 38, pp.31-50.

The European Parliament and Council of the European Union (2002) "EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector". *Official Journal of the European Communities,* 45, pp.37-47.

The European Parliament and Council of the European Union (2009) "EU Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws”. *Official Journal of the European Communities,* 52, pp.11-36.

The European Parliament and Council of the European Union (2016) “EU General Data Protection Regulation 2016 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.” *Official Journal of the European Communities,* 59, pp.1-88.

Faden, R.R. and Beauchamp, T.L. (1986) *A history and theory of informed consent*. New York: Oxford University Press.

Federal Trade Commission (FTC) (2000) *Privacy online: fair information practices in the electronic marketplace (a report to Congress).* Available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (Accessed: 14 June 2019).

Foucault, M. (1995) *Discipline and punish*. 2nd Edition. New York: Vintage Books.

Freedom of Information Act 2000, c.36. Available at: http://www.legislation.gov.uk/ukpga/2000/36/pdfs/ukpga_20000036_en.pdf (Accessed: 1 August 2019).

Freedom of Information (Scotland) Act 2002, asp.13. Available at: http://www.legislation.gov.uk/asp/2002/13/pdfs/asp_20020013_en.pdf (Accessed: 1 August 2019).

Friedman, B., Felton, E., & Millett, L. I. (2000) *Informed consent online: a conceptual model and design principles*. Available at: https://vsdesign.org/publications/pdf/UW-CSE-00-12-02_informed_consent_design_principles.pdf (Accessed: 14 June 2019).

Glasgow Libraries (n.d.) *eReading*. Available at: https://libcat.csglasgow.org/web/arena/ereading (Accessed: 18 July 2019).

*Google Spain SL v. Agencia Espanola de Proteccion de Datos* (2014) Law Reports, Queen's Bench (3rd Series), pp.1022-1080.

Gorman, M. (2015) *Our enduring values: revisited*. Chicago: ALA Editions, an imprint of the American Library Association.

*Halford v. United Kingdom* (1997) European Human Rights Reports, 24, pp.523-553.

Harris, J. (2017) "'It's just mistake after mistake' – stories from the universal credit catastrophe". *The Guardian*, 20 November 2017. Available at: https://www.theguardian.com/society/2017/nov/20/mistake-universal-credit-catastrophe-misery (Accessed: 18 July 2019).

Hsieh, H.F., and Shannon, S.E. (2005) "Three approaches to qualitative content analysis". *Qualitative Health Research*, 15(9), pp.1277-1288.

Hill Jr., T.E. (2013) "Kantian autonomy and contemporary ideas of autonomy", in Sensen, O. (ed.). *Kant on moral autonomy*. Cambridge: Cambridge University Press, pp.15-31.

Human Rights Act 1998, c.42. Available at: https://www.legislation.gov.uk/ukpga/1998/42/pdfs/ukpga_19980042_en.pdf (Accessed: 1 August 2019).

*Huvig v. France* (1990) European Human Rights Reports, 12, pp.528-547.

Information Commissioner's Office (ICO) (n.d. a) *Data protection by design and default*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (Accessed: 28 July 2019).

Information Commissioner's Office (ICO) (n.d. b) *How to access information from a public body*. Available at: https://ico.org.uk/your-data-matters/official-information/ (Accessed: 12 August 2019).

Information Commissioner's Office (ICO) (n.d. c) *What is valid consent?* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ (Accessed: 14 June 2019).

International Federation of Library Associations and Institutions (IFLA) (1994) *IFLA/UNESCO public library manifesto 1994*. Available at: https://www.ifla.org/publications/iflaunesco-public-library-manifesto-1994 (Accessed: 16 July 2019).

International Federation of Library Associations and Institutions (IFLA) (2014) *Internet manifesto 2014*. Available at: https://www.ifla.org/publications/node/224 (Accessed: 18 July 2019).

International Federation of Library Associations and Institutions (IFLA) (2015) *IFLA statement on privacy in the library environment*. Available at: https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf (Accessed: 18 July 2019).

Jabbour, V. and Rowe, H. (1995) "The proposed Data Protection Directive and the Data Protection Act 1984." *Computer and Telecommunications Law Review*, 1(2), pp.38-46.

Jaeger, P.T., Bertot, J.C., McClure, C.R. and Langa, L.A. (2006) "The policy implications of internet connectivity in public libraries". *Government Information Quarterly*, 23(1), pp.123-141.

Jensen, C. and Potts, C. (2004) "Privacy policies as decision-making tools: an evaluation of online privacy notices". *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 6(1), pp.471-478.

Kant, I. (2002) *Groundwork for the metaphysics of morals*. 2002 Edition. Binghamton: Vail-Ballou Press.

Maclean, A. (2004) "The doctrine of informed consent: does it exist and has it crossed the Atlantic?". *Legal Studies*, 24(3), pp.386-413.

*Malone v. United Kingdom* (1984) European Human Rights Reports, 7, pp.14-56.

McCoid, A. (1957) "A reappraisal of liability for unauthorized medical treatment". *Minnesota Law Review*, 41(4), pp.381-434.

McDonald, A. and Cranor, L. (2008) "The cost of reading privacy policies". *I/S: A Journal of Law and Policy for the Information Society*, 4(3), pp/543-568.

Meisel, A. (1977) “The expansion of liability for medical accidents: from negligence to strict liability by way of informed consent”. *Nebraska Law Review*¸56(1), pp.51-152.

Miles, M.B., Huberman, A.M., and Saldaña, J. (2013) *Qualitative data analysis: a methods sourcebook*. 3rd Edition. Thousand Oaks: SAGE.

Mill, J.S. (2011) *On liberty*. Urbana: Project Gutenberg.

*Montgomery v. Lanarkshire Health Board* (2015) Law Reports, Appeal Cases (Third Series), pp.1430-1471.

Moreno, J.D. and Lederer, S.E. (1996) “Revising the history of Cold War research ethics”. *Kennedy Institute of Ethics Journal*, 6(3), pp.223-237.

*Moyes v. Lothian Health Board* (1990) Scots Law Times, pp.444-451.

*Murray v. Express Newspapers* (2008) Law Reports, Chancery Division (3rd Series), pp.481-512.

Nissenbaum, H. (2010) *Privacy in context*: *technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

*NT1 v. Google LLC* (2019) Law Reports, Queen's Bench (3rd Series), pp.344-430.

Ormes, S. (n.d.) *An Introduction to Filtering*. Available at: http://www.ukoln.ac.uk/public/earl/issuepapers/filtering.html (Accessed: 1 August 2019).

Parker, R.A. and Rea, L.M. (2014) *Designing and conducting survey research: a comprehensive guide*. San Francisco: Jossey-Bass.

*Pearce v. United Bristol Healthcare NHS Trust* (1999) European Commercial Cases, pp.167-176.

.

Plante, M. (1968) “Some legal problems in medical treatment and research, an analysis of "informed consent”. *Fordham Law Review*, 36(4), pp.639-672.

Plante, M. (1978) “The decline of “informed consent”. *Washington and Lee Law Review*, 35(1), pp.91-105.

Pollach, I. (2007) “What’s wrong with online privacy policies?” *Communications of the ACM*, 50(9), pp.103-108.

Powell, R.R. (1997) *Basic Research Methods for Librarians*. 3rd Edition. Greenwich: Ablex Publishing Corporation.

*R v. Brown* (1994) Law Reports, Appeal Cases (Third Series), 1, pp.212-283.

*R v. Broadcasting Complaints Commission ex parte Granada Television Ltd* (1994) Entertainment and Media Law Reports, pp.163-169.

*Salgo v. Leland Stanford Jr. University Board of Trustees* (1957) District Court of Appeal, First District, Division 1, California. Available at: https://law.justia.com/cases/california/court-of-appeal/2d/154/560.html (Accessed: 1 August 2019).

Savage, A. and Hyde, R. (2014) “Using freedom of information requests to facilitate research”. *International Journal of Social Research Methodology*, 17(3), pp.303-317.

Schoeman, F.D. (1992) *Privacy and social freedom*. New York: Cambridge University Press.

Scottish Library and Information Council (SLIC) (2015) *Ambition & opportunity: a strategy for public libraries in Scotland 2015-2020.* Available at: https://scottishlibraries.org/media/1133/ambition-opportunity-scotlands-national-public-library-strategy.pdf (Accessed: 1 August 2019).

Scottish PEN (2018) *Libraries for privacy: a digital security and privacy toolkit*. Available at: https://scottishlibraries.org/media/2073/libraries-for-privacy-toolkit-digital.pdf (Accessed: 18 July 2019).

Semple, J. (1993) *Bentham’s prison*. Oxford: Clarendon Press.

*Sidaway Appellant v. Board of Governors of the Bethlem Royal Hospital (and Others)* (1985) Law Reports, Appeal Cases (Third Series), pp.871-905.

*Silver v. United Kingdom* (1991) European Human Rights Reports, 13, pp.582-588.

Spacey et al (2014) *Managing access to the internet in public libraries [MAIPLE].* Available at:

https://www.lboro.ac.uk/microsites/infosci/lisu/maiple/downloads/maiple-report.pdf (Accessed: 18 July 2019).

Thielman, S. (2016) "Libraries promise to destroy user data to avoid threat of government surveillance." *The Guardian*, 30 November 2016. Available at: https://www.theguardian.com/books/2016/nov/30/library-user-data-government-surveillance-donald-trump (Accessed: 18 July 2019).

*Titchener v. British Railways Board* (1983) Weekly Law Reports, 1, pp.1437-1425.

United Nations (UN) (1948) *Universal declaration of human rights*. Available at: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf (Accessed: 1 July 2019).

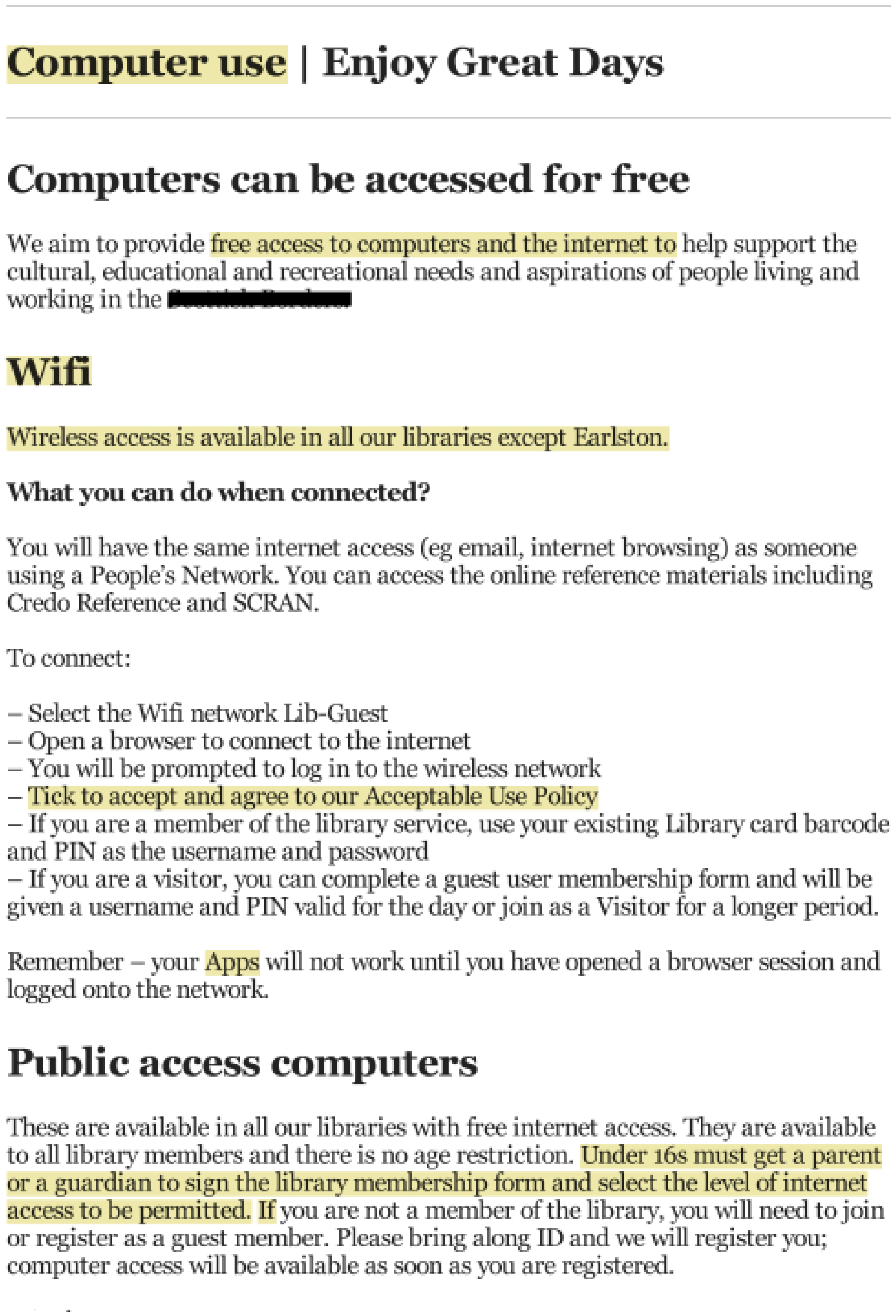
Ustaran, E. (2012) "Obtaining consent for cookies". *Privacy & Data Protection*, 12(5), pp.6-8.

Wildemuth (2016) *Applications of social research methods to questions in information and library science*. 2nd Edition. Westport: Libraries Unlimited

Williamson and Bow (2002) "Analysis of qualitative and quantitative data", in Williamson (ed.) *Research methods for students, academics, and professionals: Information management and Systems*. 2nd Edition. Wagga Wagga: Quick Print.

## APPENDIX I – WORKED EXAMPLE

### Computer Use Policy for LA01



# Computer use | Enjoy Great Days

## Computers can be accessed for free

We aim to provide free access to computers and the internet to help support the cultural, educational and recreational needs and aspirations of people living and working in the [redacted]

## Wifi

Wireless access is available in all our libraries except Earlston.

**What you can do when connected?**

You will have the same internet access (eg email, internet browsing) as someone using a People's Network. You can access the online reference materials including Credo Reference and SCRAN.

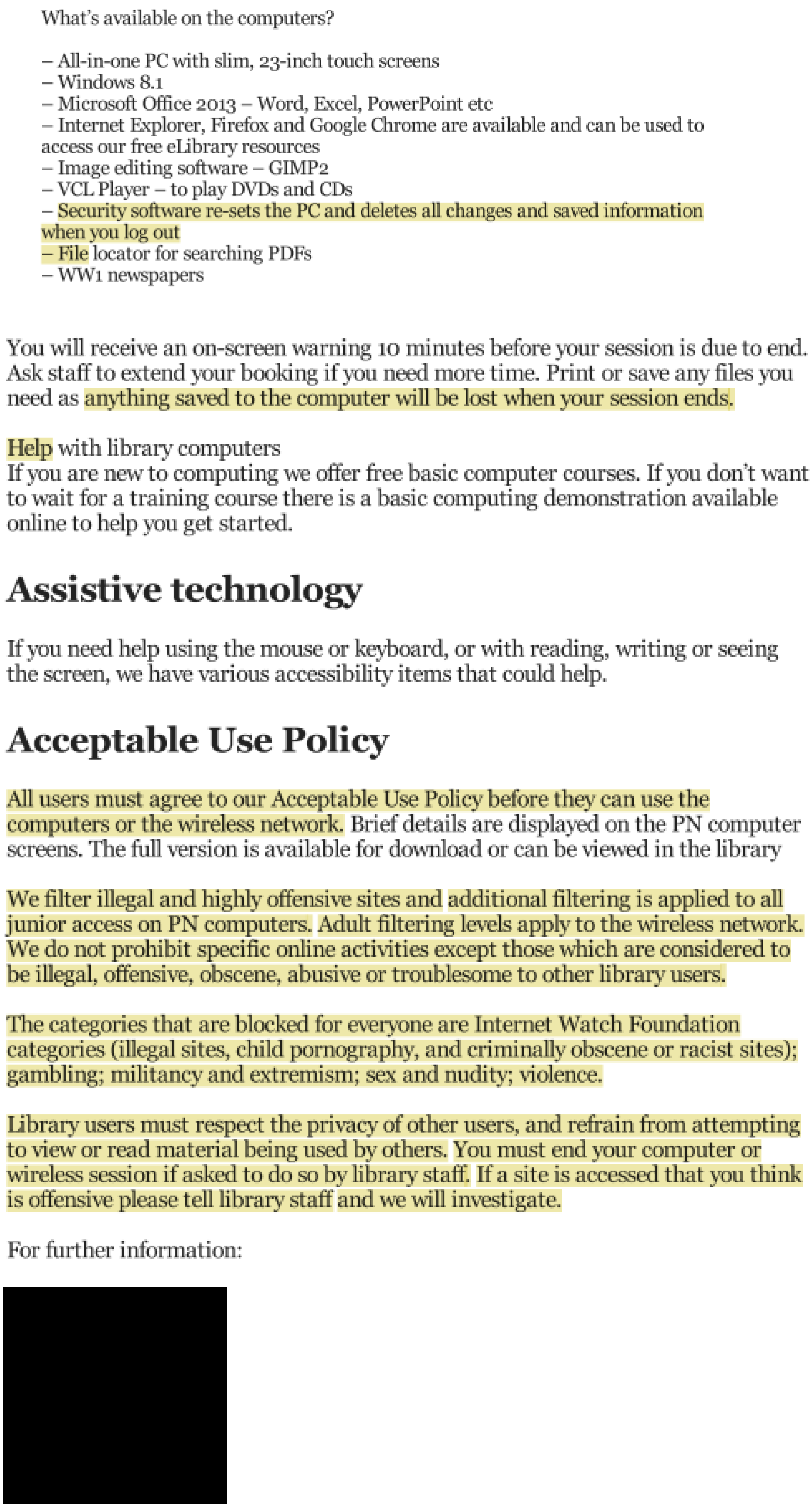
To connect:

– Select the Wifi network Lib-Guest
– Open a browser to connect to the internet
– You will be prompted to log in to the wireless network
– Tick to accept and agree to our Acceptable Use Policy
– If you are a member of the library service, use your existing Library card barcode and PIN as the username and password
– If you are a visitor, you can complete a guest user membership form and will be given a username and PIN valid for the day or join as a Visitor for a longer period.

Remember – your Apps will not work until you have opened a browser session and logged onto the network.

## Public access computers

These are available in all our libraries with free internet access. They are available to all library members and there is no age restriction. Under 16s must get a parent or a guardian to sign the library membership form and select the level of internet access to be permitted. If you are not a member of the library, you will need to join or register as a guest member. Please bring along ID and we will register you; computer access will be available as soon as you are registered.



What's available on the computers?

– All-in-one PC with slim, 23-inch touch screens
– Windows 8.1
– Microsoft Office 2013 – Word, Excel, PowerPoint etc
– Internet Explorer, Firefox and Google Chrome are available and can be used to access our free eLibrary resources
– Image editing software – GIMP2
– VCL Player – to play DVDs and CDs
– Security software re-sets the PC and deletes all changes and saved information when you log out
– File locator for searching PDFs
– WW1 newspapers

You will receive an on-screen warning 10 minutes before your session is due to end. Ask staff to extend your booking if you need more time. Print or save any files you need as anything saved to the computer will be lost when your session ends.

Help with library computers
If you are new to computing we offer free basic computer courses. If you don't want to wait for a training course there is a basic computing demonstration available online to help you get started.

## Assistive technology

If you need help using the mouse or keyboard, or with reading, writing or seeing the screen, we have various accessibility items that could help.

## Acceptable Use Policy

All users must agree to our Acceptable Use Policy before they can use the computers or the wireless network. Brief details are displayed on the PN computer screens. The full version is available for download or can be viewed in the library

We filter illegal and highly offensive sites and additional filtering is applied to all junior access on PN computers. Adult filtering levels apply to the wireless network. We do not prohibit specific online activities except those which are considered to be illegal, offensive, obscene, abusive or troublesome to other library users.

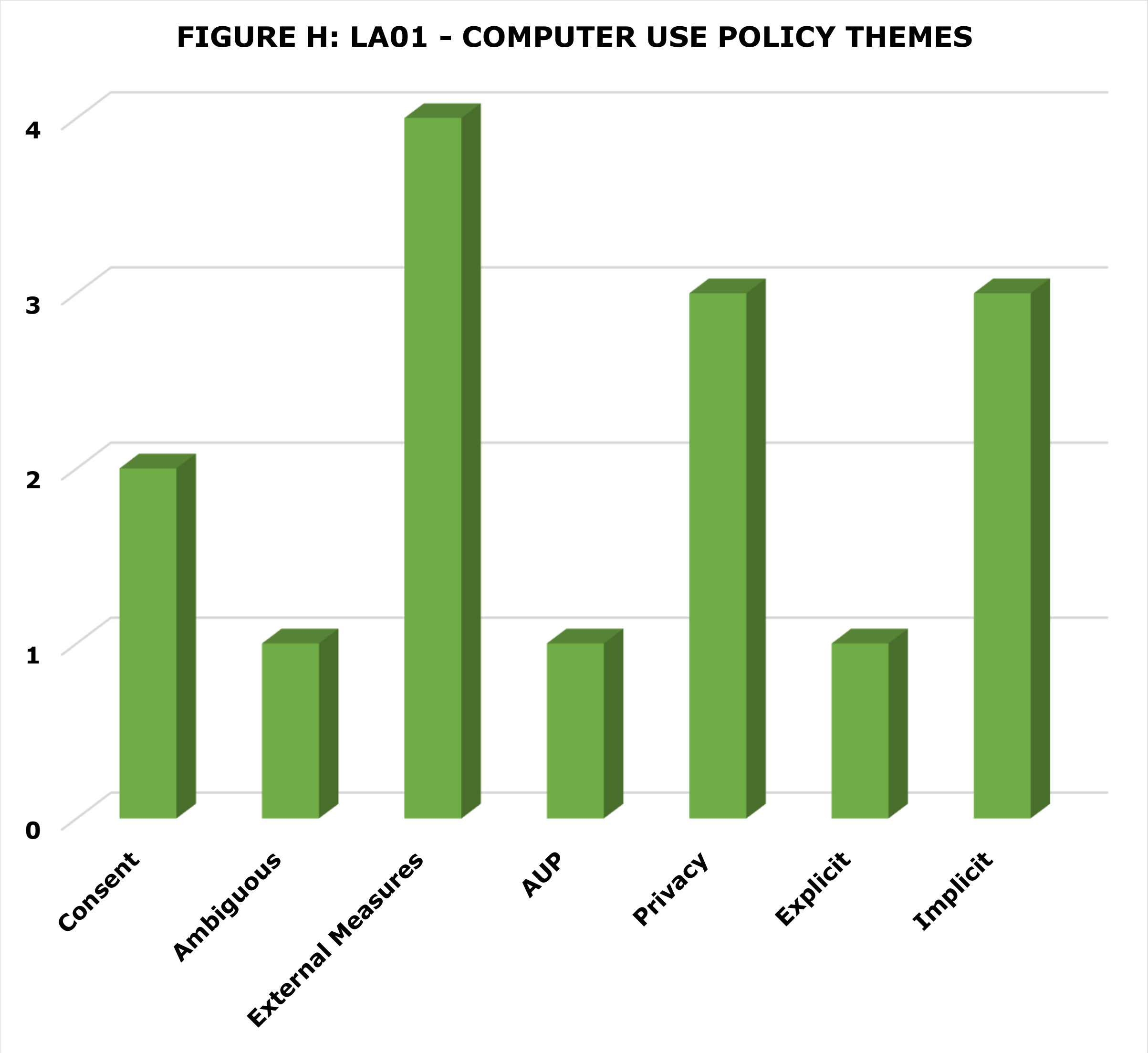
The categories that are blocked for everyone are Internet Watch Foundation categories (illegal sites, child pornography, and criminally obscene or racist sites); gambling; militancy and extremism; sex and nudity; violence.

Library users must respect the privacy of other users, and refrain from attempting to view or read material being used by others. You must end your computer or wireless session if asked to do so by library staff. If a site is accessed that you think is offensive please tell library staff and we will investigate.

For further information:

[redacted]

## Hierarchical Chart of Codes Assigned to Computer Use Policy for LA01



## APPENDIX II – FREEDOM OF INFORMATION REQUEST TEMPLATE

Dear [name of local authority freedom of information department]

I am writing to you to request information regarding your privacy policies and data protection with relation to your library services. Under the Freedom of Information (Scotland) Act 2002, I would like to request the following information from your Library Services or any other department who holds this information:

Any privacy policy or documentation with which you provide patrons of public libraries at the time of becoming members the library.

- Any privacy policy or documentation with which you provide patrons who are already members who subsequently wish to access any digital services on offer in public libraries.
- Any privacy policy, information, or guidance displayed publicly in libraries under your authority.
- Any privacy policy, documentation, or guidance with which patron-facing staff are provided in order to assist patrons with understanding or interpreting the user-facing privacy policies.
- Any documentation or information relating to any available additional user training which covers privacy when using digital services.
- Any documentation or information relating to any available additional staff training which covers privacy when using digital services.
- Any data protection policy or guidance with which you provide staff.
- Any data protection policy or guidance with which you provide patrons.

Please provide the information in digital form where possible. Where possible, could you please also indicate whether the information given to patrons is given to them to keep (or made available for them to do so, for example, online) or whether the information is only shown to the patron at the time of joining.

Please let me know if it is not possible to provide this information for reasons of cost, per s.12 of the aforementioned act. In that event, please, if possible, provide advice on refining my request, per s.15 of the same act.

Thank you for considering my request. I hope to hear from you soon. If any clarity is needed on any of the matter mentioned above, please let me know by email or phone – my contact details are below.

Kind regards,

Suzanne Connor

Email: suzanne.connor.2018@uni.strath.ac.uk