mEducation

Safeguarding, Security and Privacy in Mobile Education

Executive Summary

An increasing number of educators in many countries are experimenting with, or embedding into their practice, the use of mobile technologies to deliver or support learning. This practice can make learning and assessment more personal, convenient, attractive and engaging for learners as well as reduce the physical strain of carrying around heavy books and files and improve learner attendance and success. Benefits to institutions can include more flexible delivery of learning, reduced costs, improved reputation for innovation and modernity, improved communication with students and easier differentiation of teaching to meet students' varied abilities, needs and preferences.

However, some educators and institutional managers are reluctant to, or worried about, introducing the use of mobile technologies for teaching and learning and many schools still have policies banning the use, or even the presence, of mobile phones on their premises.

The reasons for this reluctance are varied. Institutional management may worry about the potential for negative reactions from parents, negative publicity resulting from the prejudices of more conservative elements of the media, or problems arising from misuse of the technologies. Management and teaching staff may be concerned about the possibility of younger students, and vulnerable adults, accessing inappropriate online materials or communication. They may also worry about alleged health risks, the use of mobile phones for bullying and students facing an increased risk of theft. IT staff at educational institutions may be concerned about increased support workload and increased threats to system and data security, especially if students are allowed to use their own mobile devices to access institutional services. Teaching staff may worry about the functionality of mobile technologies, and the systems they provide access to, distracting students from their learning tasks and adversely affecting their behaviour. Some teachers may also feel very unsure about and threatened by the introduction of new technology, especially when students seem to be more confident and knowledgeable users of this technology than the teachers.

These concerns can be a barrier to the introduction of mobile technologies into education thus preventing institutions and students from realising the benefits of using these technologies.

However, there is now a substantial amount of available knowledge, expertise, experience and research evidence which institutions and teaching staff can draw upon to help them to avoid, or mitigate the impact of, the risks they may fear and maximise the benefits offered by the technologies. This includes the unique knowledge, expertise and experience mobile network operators have amassed as a result of developing and operating the hugely scalable, secure systems that enable mobile communication.

This publication summarises the main concerns of educators in the areas of safeguarding, privacy and security, provides advice for addressing these concerns and signposts further information and sources of advice.

Contents

1. Introduction

1.1 Purpose and intended audience

The purpose of this paper is to inform and assist, in the specific context of safeguarding, security and privacy, the following organisations and individuals:

- Educational institutions involved in, or considering, implementing mobile learning
- Mobile technology and connectivity providers supporting or working with these institutions
- Companies such as publishers, software developers, solutions providers involved in implementing mobile solutions for education and training
- Local, regional and national educational policy makers

1.2 The mobile technologies used for education and training

Mobile technologies used in education and training include mobile phones, smartphones, PDAs, MP3/MP4/media players, e-Book readers (e.g. Kindle), Ultramobile PCs (UMPCs) and netbooks, tablet PCs (e.g. iPad, Galaxy Tab), hybrid tablet/smartphone devices (e.g. Galaxy Note), handheld gaming devices (e.g. Sony PSP and Playstation Vita, Nintendo DS), handheld GPS devices, connected cameras, classroom voting devices and specialist portable technologies used in science labs, engineering workshops or for environmental or agricultural study.

A few models of these technologies have been specifically designed for use in education (e.g. the one laptop per child (OLPC) initiative[1], the Intel Convertible Classmate[2], the Aakash tablet[3]) but in most cases educators are using available consumer technologies.

1.3 What is mobile learning

A broad definition of mobile learning is "The exploitation of ubiquitous handheld technologies, together with mobile and wireless networks, to facilitate, support, enhance and extend the reach of teaching and learning."

Mobile learning involves connectivity for downloading, uploading and/or online working via mobile networks, wireless networks, or both, and linking to institutional systems e.g. learning management systems (LMS), managed or virtual learning environments (MLE/VLE) and management information systems (MIS).

Mobile learning can take place at any time in any location, including traditional learning environments such as school, college and university classrooms, lecture theatres, libraries, workshops and canteens as well as in workplaces, learners' homes, community locations, field trip locations, the countryside and public transport. Learners include children, students and adults and their learning may result in formal qualifications or the acquisition of specific skills or be motivated by a hobby or interest.

1 http://one.laptop.org/

2 http://www.intel.com/pressroom/kits/classmatepc/

3 http://www.bbc.co.uk/news/world-south-asia-15180831

Some definitions of mobile learning include the use of laptop computers for learning. The advent of 10 inch netbooks and tablets together with the great variety in the size and weight of wireless enabled, and increasingly 3G enabled, laptops is seen by some commentators as eroding the distinction between laptops and mobiles and therefore also eroding the position of mobile learning as a distinctive sub-set of 'technology enhanced learning'. Some researchers (e.g. Gi-Zen Liu and Gwo-Jen Hwang, 2010[4]) place the use of connected and location aware mobile technologies within the concept of 'ubiquitous learning'.

1.4 What is mobile education

'Mobile Education' is an extension of 'mobile learning', including the full range of opportunities mobile technologies and systems offer for improving formal learning, teaching, assessment and educational administration and management. Mobile education incorporates access to e-books and online learning materials and systems, student/student collaboration, student/tutor communication, evidence collection, e-portfolios, e-assessment, attendance monitoring, task planning, curriculum and device management.

1.5 The mobile education context

The use of mobile technologies in education is increasing rapidly in terms of: the number of learners engaged in mobile learning; the number and variety of mobile technologies used; and the number of subjects and contexts.

Following many years of experimentation and trials, the adoption of mobile technologies for use in education is rapidly accelerating and is becoming an accepted and integral part of delivery in some areas of the education sector in an increasing number of countries. This trend is enabling institutions:

- To modernise their offer to learners
- To provide more flexible, differentiated, personalised and convenient learning opportunities
- To improve the authenticity, efficiency and relevance of vocational learning and assessment
- To improve the quality, immediacy and efficiency of off-site learning support

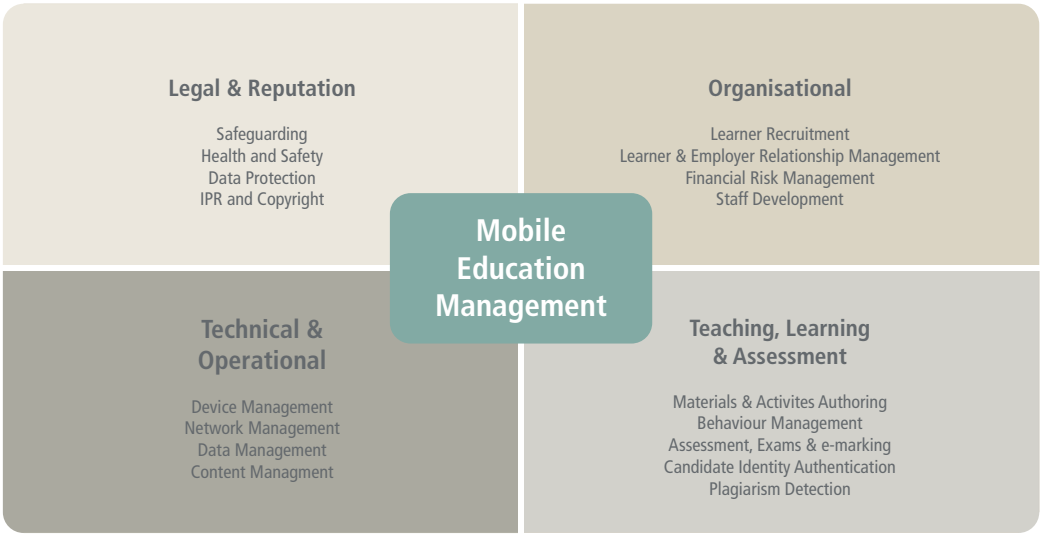
However, it also introduces management and administrative challenges to those already implied by institutional provision of static technologies to support teaching and learning.

In addition to pedagogical questions concerned with how the technologies can be used to support teaching, learning and learner achievement, institutions need to address a variety of Mobile Education Management issues.

These challenges can be technical, legal, related the running of the institution as a business or related to the administration of teaching, learning and assessment (Figure 1).

4 Gi-Zen Liu and Gwo-Jen Hwang, 2010, "A key step to understanding paradigm shifts in e-learning: towards context-aware ubiquitous learning" in British Journal of Educational Technology Volume 41, Issue 2, pages E1–E9, March 2010, http://onlinelibrary.wiley.com/doi/10.1111/j.1467-8535.2009.00976.x/full

Figure 1: Mobile Education Management



Source: GSMA 2012

1.6 The focus of this report

The focus of this paper is a sub-set of the challenges associated with Mobile Education Management specifically related to education sector stakeholders' concerns in the areas of safeguarding young or vulnerable learners and protecting the privacy and security of individuals, data, systems and equipment.

A key concern for educationalists, policy makers and parents is ensuring that children and vulnerable adults can use mobile technologies, and the online services and communication accessed through these technologies, safely.

While questions about the social impacts of children's use of mobile phones are frequently raised in education and in wider society, the trend towards increasing usage of these and of other handheld technologies looks set to continue. In this environment, both educators and mobile operators have recognised the need to adopt a consistently responsible approach in order to protect and support younger and more vulnerable users.

Mobile operators and GSMA have a number of initiatives designed to address these issues as well as partnering with wider stakeholder to address these concerns collaboratively. In particular the GSMA is a member of:

- Teachtoday[5], the definitive online resource for teachers in Europe, which is focused on the responsible and safe use of new communications technologies
- The Family Online Safety Institute (FOSI)[6], which "works to make the online world safer for kids and their families by identifying and promoting best practice, tools and methods in the field of online safety, that also respect free expression"
- ITU, the UN agency for information and communication technologies who are responsible for the Child Online Protection (COP) global initiative[7] (see section 2.1 for further information).

5 http://www.teachtoday.eu/

6 http://www.fosi.org/

7 http://www.itu.int/osg/csd/cybersecurity/gca/cop/

GSMA and its members also address privacy issues related to consumers' use of mobile technology. The rapid convergence of the mobile and web industries along with the growth of smartphones and innovative applications and services are bringing significant benefits to consumers and society. However these welcome developments are also re-shaping the online privacy landscape and are leading to the emergence of new privacy challenges across the mobile ecosystem. GSMA has identified two key challenges for the industry and for developers of systems and Apps as the need to:

- Identify mobile-friendly ways of helping users make informed decisions about their information and privacy
- Ensure user privacy is respected and protected by those designing and building the services and applications of tomorrow

These issues are addressed through GSMA's mobile privacy initiative and further information can be found at www.gsmworld.com/mobileprivacy.

1.7 Institution issued or student owned mobile technologies?

The nature of, and the solutions to, some of the issues discussed in this paper can differ according to which of two very broad use cases apply i.e. whether students are using mobile technologies provided by an educational institution or using their own personally owned mobile technologies to organise their learning and to access learning resources, systems and support. Dependent upon which of these cases applies institutions will have differing responsibilities and will need to develop different policies and processes.

Early mobile learning projects, including projects and initiatives funded by institutions, governments and charities, usually provided participating students, and in some cases teachers and other staff, with mobile devices. However a recent trend in many countries is for institutions wishing to implement or expand mobile education to enable and facilitate students to use their own mobile devices. In some cases students or their parents can purchase their devices via institutional schemes which may offer discounts or the ability to pay in instalments. This trend is being driven by a number of factors including:

- More widespread ownership of mobile technologies
- More common ownership of more sophisticated, Internet enabled devices
- More ubiquitous mobile and wireless networks
- Student preferences for using their own familiar and personalised devices
- Student reluctance to carry extra devices
- A desire to make mobile education initiatives and projects more cost effective and more future-proof by leveraging student owned technologies

However, BYOD (bring your own device) or BYOT (bring your own technology) strategies are not uncontroversial especially in schools. For example one influential educator and blogger (Stager, S, 2011[8]) provoked much debate by asking "BYOD – Worst Idea of the 21st Century?", whilst an author who blogs under the name "the innovative educator" has written "7 Myths about BYOD debunked" (Neilson, L, 2011[9]).

8 Stager, S, 2011, "BYOD – Worst Idea of the 21st Century?", Stager-to-Go blog, http://stager.tv/blog/?p=2397

9 Neilson, L, 2011, "7 Myths About BYOD Debunked", the Journal.com, http://thejournal.com/articles/2011/11/09/7-byod-myths.aspx

Issues raised by some educators and IT managers, which others dismiss or suggest solutions to, include concerns that BYOD (as opposed to the strategy of institutions providing technology) might:

- Deepen the digital divide[10]
- Result in lessons geared toward the weakest device
- Be more likely to cause student distraction
- Require teaching staff to become experts in all the different technologies students own
- Put students at risk by enabling unrestricted access to the Internet
- Require more development work to ensure software and apps work on many different devices
- Provide an inferior technology platform, compared with more powerful computers

When considering whether to introduce BYOD, institutions need to have clear objectives based on the benefits they hope to achieve and plans for how risks will be addressed and minimised.

Objectives should be focussed on desired educational outcomes and improvements in the student experience. If objectives include a desire to make delivery of learning more cost effective, care needs to be taken to ensure a focus on effectiveness not merely on cost reduction to avoid adverse impact on the quality of provision. Stager expresses a fear that BYOD may contribute to "the growing narrative that education is not worthy of investment" and warns that important educational decisions should not be based solely on price.

Possible negative consequences can be mitigated by identifying risks and planning strategies to address these. If, for example, inequality in devices owned by students is a cause of concern, strategies can include helping students with purchasing by negotiating discounts with suppliers and enabling payment in instalments. Loan arrangements can also be put in place, probably administered by the library or learning resource centre. Concerns about younger students having unrestricted access to the Internet can be addressed by obtaining parental agreement to control access by installing mobile device management software on students' mobiles.

10 The term digital divide is frequently used to refer to the gap between people with access to information and communications technologies and people who have limited or no access to it. Broader definitions of the term include not only the imbalance in physical access but also inequality in the acquisition of the resources and skills required to use it. The digital divide is commonly linked to inequality related to gender, age, ethnicity, geographic location, income or education level.

2. Safeguarding

In many countries safeguarding is a legal responsibility where learners are under 16 years of age, or identified as vulnerable adults, and there is a general duty of care to all clients and staff of educational institutions.

Safeguarding challenges include the need to:

- Control access to inappropriate material and communication e.g. violent, pornographic or age inappropriate content, grooming and bullying
- Avoid exposing learners to health and safety risks

Educational institutions' duty of care to their students, and their employees, also includes protection from bullying or harm by other students or employees.

A broader interpretation of safeguarding may include ensuring that teaching and learning methods do not have an adverse effect upon students' learning experiences, achievement or general wellbeing. In this context some institutions and teachers may wish to include under safeguarding the need to ensure that the introduction of any new approach or technology does not result in students being distracted from their learning activities or affected by any resultant bad behaviour by other students.

However, there may be a tendency for some teaching staff, who are uncomfortable with the idea of using mobile technologies for teaching and learning, to use the need to protect students as an excuse for restricting use. Whilst some risks to young or vulnerable people's wellbeing, e.g. so called "cyber bullying", may be better addressed by educating the victims and the perpetrators rather than seeking to ban specific technologies or online services.

2.1 Controlling access to inappropriate content and communication

Most relevant to: schools, colleges, under 16s, vulnerable adults, with some implications for others

Solution type (policy, technical, culture change or staff development): policy, technical, culture and staff training

Criticality: *"Potential Showstopper"*, if education providers are not confident that young or vulnerable learners can be protected from really inappropriate content. *"Potential to discourage/restrict use"*, if educators are very concerned about genuine or perceived risks.

Description and discussion

Having the ability to restrict access to illegal and inappropriate content is a critical requirement for mobile education in order to ensure children's safety and satisfy the legal duty of care under which most educational institutions operate. There are several separate issues to be addressed here:

- Illegal content which should not be available to anyone
- Content that is legal but inappropriate for children e.g. pornography, gambling sites
- Inappropriate online communication with young people e.g. victim grooming

Institutions may also have concerns about systems or websites that are suitable for children but may be considered a distraction or nuisance in the learning environment e.g. social networks, computer games.

Institutional controls

Where students are using institutional networks, policies and systems, including firewalls, filtering and virus control, may already be in place to safeguard them from inappropriate content and communication as a result of institutions' experience of providing access to the Internet via desktop computers. These safeguards should be extended to cover students using mobile devices connecting to the Internet via the institution's WiFi. However, when introducing mobile technologies which can also be used outside of the institution, via either home WiFi or mobile networks, institutions need to consider what controls are necessary to implement or advise parents to implement. Implementing controls on-device is also an option for devices provided to the learner by the institution so they are in place regardless of which network is being used.

Illegal content

In many countries, access to illegal content is blocked by mobile operators through a pro-active industry initiative, called the Mobile Alliance against Child Sexual Abuse Content[11]. The objective of the Alliance is to obstruct the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content. Members of the Alliance have agreed to "work to prevent access to websites identified as hosting child sexual abuse content" and "implement Notice and Take Down processes to enable the removal of any child sexual abuse content posted on their own services, while supporting and promoting 'hotlines' for customers to report child sexual abuse content discovered on the Internet or on mobile content services."

Age inappropriate content

In some countries, operators take a pro-active approach with regard to inappropriate content. For example, in the UK all operators subscribe to a Code of Practice for the self-regulation of content on mobiles[12]. This code of practice does not cover traditional premium rate voice or premium rate SMS services or peer to peer communications but does combat bulk and nuisance communications. Operators also restrict access to content classified as "18+" by content providers, according to the Independent Mobile Classification Board (IMCB) classification framework, until customers have verified with their operator that they are over 18.

There are a number of activities going on within industry, within countries and at the European level to address issues related to child online safety and specifically access to age appropriate content.

For example in December 2011, the European Commission announced the launch of a pan – ICT industry CEO coalition. Companies involved include several leading European mobile operators. Priority actions for the Coalition include "making it easier to report harmful content, ensuring privacy settings are age-appropriate, and offering wider options for parental control, reflecting the needs of a generation that is going online at an increasingly young age" (EU, 2011[13]). This Coalition sits alongside the ICT principles, another pan-industry initiative which seeks to enhance online safety for children and young people.

Regarding age-appropriate settings, a common complaint from teenage mobile users, e.g. 16 and 17 year olds, is a perception that much content categorised as only suitable for over 18s is not really unsuitable for users of their age. This can become an issue for teachers who may wish to use resources they consider suitable for their learners but find them blocked as content providers have categorised them as 18+.

11 http://www.gsma.com/mobile-alliance/

12 http://www.mobilebroadbandgroup.com/documents/mbg_content_code_v2_100609.pdf

13 EU December 2011 press release http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1485&format=HTML&aged=0&language=EN&guiLanguage=en

There may be scope for mobile operators to assist in addressing this issue by developing improved, more flexible and sophisticated internet filtering tools and processes.

Inevitably there has been much debate about how best to verify that a customer using mobile services is aged 18 or over. Some operators accept ownership of a credit card used to pay for mobile services as an indication that the holder is 18 or over. Others require customers to bring proof of identity to one of the operator's shops, arguing that many services used by under 18s are paid for using a parent's credit card. A small charge is often made for using a credit card to verify age as this causes an item to appear on the card owner's credit card bill thus alerting them if they were unaware that their card was being used.

Japanese mobile operators, having themselves verified the age of their customers, provide an Age Verification Service to providers of online services and also providers of other age restricted products including cigarettes and alcohol sold through vending machines (Birch, D, 2011[14]).

Age inappropriate communication control

A related concern is the need to verify the age of people communicating with young learners via social networking sites. One example of how to address this issue is Project Isis[15], led by Lancaster University in the UK. A software package was developed which estimates a person's age and gender using language analysis techniques. The aim was that this could be used to help police and law enforcement agencies detect an adult in a chatroom masquerading as a child as part of the "victim grooming" process. The system can also build general language profiles of paedophiles and paedophile groups to assist police in identifying them online. The language analysis software developed within the project is commercially available via a spin-off company Isis Forensics[16] who have also developed an iPhone App with the aim of empowering children to protect themselves when they are online by using the App to determine if the person they are communicating with is actually who they claim to be.

Websites considered a distraction from learning

Whether to prevent student access to websites which might distract from learning or cause behavioural problems is the subject of much debate in Education. Discussion revolves around:

- Whether preventing access is more or less desirable or effective than educating students about safe and responsible internet use
- Whether institutions should by default trust students and staff, and only apply sanctions to transgressors, or impose blanket bans

Many institutions and companies operate a Blacklisting system whereby websites or categories of websites deemed to be inappropriate are blocked for all users but can be unblocked for individuals if required. Whitelisting' or 'Walled Garden' services are alternative approaches designed for educational institutions. These 'involve identifying websites considered to be acceptable, or of educational value, and allowing access to only these sites. Many students, and some teachers, consider this approach too restrictive for all but the youngest children. It also raises important practical questions, for example who decides what sites should be included and excluded? How is the list kept up to date?

14 Birch, D, 2011, "Aging problem", Digital Identity Blog, http://digitaldebateblogs.typepad.com/digital_identity/2011/01/index.html

15 http://www.comp.lancs.ac.uk/isis/

16 http://www.isis-forensics.com/childprotection/solution/solution.php

Whilst attractive to institutions in terms of managing risk, it has been suggested that Walled Gardens can result in more rather than less risk to learners as:

"…teachers and management perceive that the network is locked down and thus safe, they don't need to worry about informing the learners about e-safety and digital identity. Of course once that learner goes home to their unlocked home internet, their smartphone, their 3G dongle, a friend's computer… they have no concept of how to act responsibly and safely online and as a result put themselves at risk….." (James Clay, 2010[17])

Ofsted inspectors have stated that "*Students are safest using the internet when they are trusted to manage their own risk*" (Ofsted 2010[18])

Walled Gardens can have educational drawbacks and present operational challenges:

"The safe search facility [provided by the network operator] means that young learners are protected from access to inappropriate material. However, the challenge here is to ensure that searches are not too restricted and that learners have access to sites such as major news groups and popular social networks particularly as the education sector is still learning how to utilise these sites in an educational context."
Raja Habib, Partnership Manager, MoLeNET LifeWise project.

Some teaching staff involved in the early stages of the MoLeNET 'Learning2Go Further' project became very frustrated by being unable to access websites they wished to use in teaching and this acted as a disincentive to their engagement with mobile education:

"The number of URLs accessible by the devices was found to be relatively low and did not meet the needs of staff. This has interrupted the delivery of training beyond initial device familiarisation in some organisations and has led to some staff feeling that they have been unable to incorporate devices into teaching and learning practices due to the limited Internet access."[19]

Sources of information and advice

GSMA

GSMA leads or participates in several initiatives which are designed to protect children and young people using mobile phones.

Age sensitive content:[20] Toolkit for mobile operators to support the responsible delivery of age-sensitive commercial content

- **European Framework for Safer Mobile Use by Younger Teenagers and Children:**[21] A self-regulatory initiative by the mobile industry, which makes recommendations to ensure that younger teenagers and children can safely access content on their mobile phones

- **The EU ICT Coalition for a Safer Internet for Children and Young People:**[22] GSMA, along with other leading trade associations is supporting a new ICT Coalition which is expected to launch in 2012 a set of European wide principles aimed at enhancing online safety for children. The ICT Coalition and its principles mark a unique step in the evolution of industry self-regulation. It brings together for the first time many key industry players from across an increasingly wide and converging communication and internet market.

17 Clay, J, 2010, "to block or not to block", e-Learning Stuff, http://elearningstuff.net/2010/02/15/to-block-or-not-to-block/

18 Ofsted, 2010, http://www.ofsted.gov.uk/news/students-safest-using-internet-when-they-are-trusted-manage-their-own-risk

19 Learning2Go Further", 2008, https://www.wolverhampton-engage.net/sites/anonymous/Learning2Go/Downloads/Forms/AllItems.aspx

20 http://www.gsma.com/age-sensitive-content/

21 http://www.gsma.com/european-framework/

22 http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm

The ICT Principles aim to ensure that signatories will aspire to the:

- Development of innovative approaches to enhance safe and responsible use by children and young people
- Empowerment of parents and carers to take action to engage with, and protect, their children
- User awareness of ways to ensure safety online and responsible behaviour towards others
- Provision of easily accessible, clear and transparent information
- Awareness of how – and to whom – to report abuse and concerns

- **Teachtoday:**[23] The definitive online resource for teachers in Europe, which is focused on the responsible and safe use of new communications technologies. Teachtoday provides information and advice for teachers, head teachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies. This includes advice about bullying. Founding partners of Teachtoday include European Schoolnet (EUN) a network of 31 Ministries of Education in Europe dedicated to supporting schools in the effective and responsible use of technology in learning, GSMA, O2, Orange, Telecom Italia, Deutsche Telekom and Vodafone, as well as several other leading technology companies.
- **Family Online Safety Institute (FOSI):**[24] GSMA is a member of FOSI (Natasha Jackson, GSMA's Head of Content Policy, is a member of the FOSI Board), which "works to make the online world safer for kids and their families by identifying and promoting best practice, tools and methods in the field of online safety, that also respect free expression".
- To gain a better understanding of how children use their mobile phones across the world, GSMA has collaborated with NTT DOCOMO on a multiyear research project comparing children's use of mobile phones in different countries[25]. The 2010 report "Children's Use of Mobile Phones and Personal Relationships - An International Comparison" was published in June 2010 with NTT DOCOMO's Mobile Society Research Institute (MSRI)[26], and compares mobile phone use by children in six countries at different stages in their development - Japan, Korea, Cyprus, China, India and Mexico. The Children's Use of Mobile Phones - An International Comparison 2011 report provides a detailed picture of mobile phone use by children from the age of eight to 18, following research conducted with more than 3,500 pairs of children and parents in Japan, India, Paraguay and Egypt.

UK

- **Ofsted**[27]
- **Get safe online**[28]
- **Child Exploitation and Online Protection Centre**[29]
- **UK Council for Child Internet Safety**[30] which brings together over 170 organisations, including major mobile operators and is jointly chaired by the Department for Education and the Home Office
- **The Byron reports** (2008, 2010)[31]
- **The Safe Network**[32] - Jointly managed by NSPCC, Children England and Child Accident Prevention Trust (CAPT), created as a result of the UK Department for Children Schools and Families 2009 Staying Safe Action Plan[33]

23 http://www.teachtoday.eu/

24 http://www.fosi.org/cms/

25 http://www.gsma.com/understanding-usage-of-mobile-by-young-people/

26 http://www.moba-ken.jp/english

27 http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies

28 www.Getsafeonline.org

29 http://ceop.police.uk/

30 http://www.education.gov.uk/ukccis

31 Byron, T, 2008, "Safer Children in a Digital World", and 2010, "Do we have safer children in a digital world?"

32 http://www.safenetwork.org.uk/help_and_advice/Pages/safety_online.aspx

33 https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00151-2008.pdf

European Union

- **Kidsonlinenet research project:**[34] social networking safety summary findings
- **Insafe:**[35] the European network of Awareness Centres promoting safe, responsible use of the Internet and mobile devices to young people

USA

- **WiredSafety.org:**[36] is a US charity operating worldwide. It originated in 1995 as a group of volunteers rating websites and now provides one-to-one help, information and education to Internet users of all ages on Internet and interactive technology safety, privacy and security issues. These services are offered through unpaid volunteers who administer specialised websites, resources and programmes.
- **Harvard University, Berkman Center for Internet and Society, The Youth and Media Policy Working Group:**[37] this group explores policy issues that fall within three substantive clusters that emerge from youth's information and communications technology practices: Risky Behaviors and Online Safety; Privacy, Publicity and Reputation; and Youth Created Content and Information Quality.

United Nations

- **ITU:**[38] the UN agency for information and communication technologies

2.2 Mobile bullying

Most relevant to: schools, colleges, under 16s, vulnerable adults, with some implications for others

Solution type (policy, technical, culture change or staff development): policy, culture, staff training, learner guidance, advice and support

Criticality: "*causes concern*" and "*potential to discourage/restrict use*" if teachers are particularly concerned

Description and discussion

Some teaching staff and managers of educational establishments express concerns that mobile devices can be used for bullying other learners and teachers.

Unfortunately technology, including mobile technologies, has enabled the old fashioned school, or office, bully to increase the reach, intensity and longevity of their activities. Bullying may be online and therefore delivered via either desk top or mobile technologies or may use the functionality of mobile technologies e.g. photographing or videotaping peers or teachers for circulation, posting and ridicule.

34 http://media.education.gov.uk/assets/files/pdf/r/14%20%20%20social%20networking%20age%20and%20privacy.pdf and http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf

35 http://www.saferinternet.org/web/guest/home

36 http://www.wiredsafety.org/

37 http://cyber.law.harvard.edu/research/youthandmedia/policy

38 http://www.itu.int/osg/csd/cybersecurity/gca/cop/so-whats-cop.html and http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/industry/industry.pdf

The use of mobile technologies for educational purposes probably does not increase the risk that may already exist as a result of learners' personal ownership of mobiles.

Investing time and effort in education and communication with young people on the issue of bullying can help. Technology alone cannot provide the solution, young people need to have the tools and knowledge to enable them act appropriately online and to cope with difficult situations.

Institutions should also re-visit their existing anti-bullying policies and strategies to ensure that they are robust enough to cope with the use of new technologically facilitated bullying methods.

Sources of information and advice

- Childline[39]
- Kidscape[40]
- Childnet's 'The Digizen' website[41]
- Wired Kids Inc's 'Stop Cyberbullying' website[42]
- Cybermentors[43] – a website for children mentoring each other concerning online bullying

2.3 Device functionality and access to websites or services considered to be a distraction or potentially problematic

Most relevant to: schools, colleges, under 16s, vulnerable adults, with some implications for others

Solution type (policy, technical, culture change or staff development): policy, technical, culture and staff training

Criticality: "*Potential to discourage/restrict use*", if educators are very concerned about perceived distraction or behaviour risks

Description and discussion

Some educators would like to be able to disable, within institutions or within classrooms, some device functionality (e.g. the ability to make phone calls or send texts) which they perceive as likely to distract from learning or lead to behavioural issues. Some institutions are also concerned about the use of cameras in mobile devices combined with social networking websites to bully or embarrass learners or teachers. Some employers of work-based learners do not allow devices with cameras on their premises as they are concerned about the potential for industrial espionage.

There is much debate within education about whether the ability to temporarily disable such functionality, or even the right to ban mobile technologies, is needed or whether concerns can be adequately addressed by acceptable use agreements and updated teacher training and continuing professional development in classroom behaviour management.

39 http://www.childline.org.uk/Explore/Bullying/Pages/CyberBullying.aspx

40 http://www.kidscape.org.uk/childrenteens/cyberbullying.shtml

41 http://www.digizen.org/

42 www.stopcyberbullying.org

43 http://cybermentors.org.uk/index.php?option=com_frontpage&Itemid=1

If institutions feel they need to apply technical controls, possibilities include:

- The use of Apps to provide access to limited and specific internet pages on mobiles instead of Internet access via a browser
- Limiting of device functionality, or services accessible on mobile devices, permanently or in specific locations at specific times

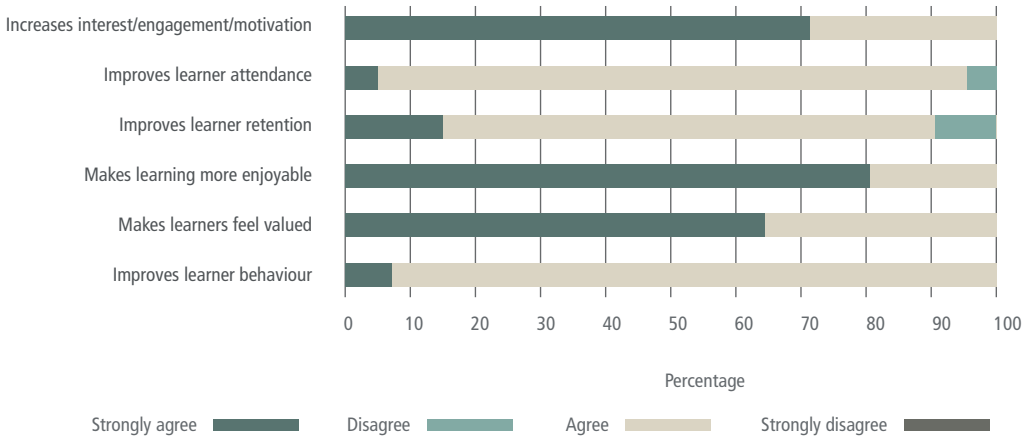
Some institutions have also taken the decision to use iPods and other media players and tablets rather than smartphones for learning partly because students cannot use these devices to make phone calls or send texts (although Voice over Internet Protocol (Voice over IP, VoIP) services, e.g. Skype or Oovoo, might potentially still be used unless blocked).

In recent years in the UK many educational institutions have experimented with the use of previously banned handheld technologies, including mobile phones and games devices (i.e. Nintendo DS and Sony PSP) for learning.

Research carried out by institutions taking part the UK MoLeNET initiative[44] found that whilst initially many teachers raised concerns about possible negative effects on student behaviour in practice these fears were generally not realised and in some cases student behaviour improved[45].

College staff leading MoLeNET projects in year 3 provided largely positive feedback on the impact of the use of mobile technologies on students' engagement, behaviour, attitudes and retention[46] (Figure 2).

Figure 2: MoLeNET Year 3 Projects Feedback on the Impact of Mobile Learning on Learner Engagement, Behaviour, Attitudes and Retention



Source: Attewell J et al 2011

44 www.molenet.org.uk

45 Attewell J et al, "The impact of mobile learning, examining what it means for teaching and learning", LSN 2009, ISBN: 978-1-84572-820-5 and "Modernising education and training, Mobilising technology for learning", LSN 2010, ISBN: 978-1-84572-972-1

46 Attewell J et al, "Mobile learning news: Proven effective, sustainable m-learning, key mes sages from 3 years of MoLeNET", LSN 2011, ISSN 1473-1685

Some institutional policies related to banning, blocking or filtering of mobile devices, device functionality, websites, content and communication are designed to control the use of technologies perceived as potentially disruptive. Although educators and institutional managers quite correctly wish to protect their learners and the reputation of their institutions some policies are also motivated by a fear of losing control and of their traditional roles, processes, culture and authority being challenged.

Some researchers have described mobile technologies as "disruptive" in education in ways that are positive. The term disruptive technology was first coined in by Clayton Christensen in 'The Innovator's Dilemma'[47]. Christensen suggested that innovations were either 'sustaining' or 'disruptive'. A 'sustaining' innovation being one which improves performance in line with the demands of mainstream users, whilst a 'disruptive' innovation has characteristics that users may not initially want. However, disruptive innovations have the potential to drastically change the way users connect, engage, and relate with the world and can transform society, which can be very beneficial hence the title of "the innovator's dilemma".

An increasing number of educators are recognising the potential of mobile technologies for teaching and learning and speaking out against the previously widely accepted view that mobile phones should be banned in schools. One group of teachers have written an article entitled "10 Proven Strategies to Break the Ban and Build Opportunities for Student Learning with Cell Phones" (Engel, G et al, 2010[48]) which provides other teachers with advice as well as links to useful evidence to support arguments for the use of mobile in schools and useful tools to assist the process of getting started.

Engel et al advise teachers who wish to change the system to carefully plan their strategy and advise them to follow a series of steps including:

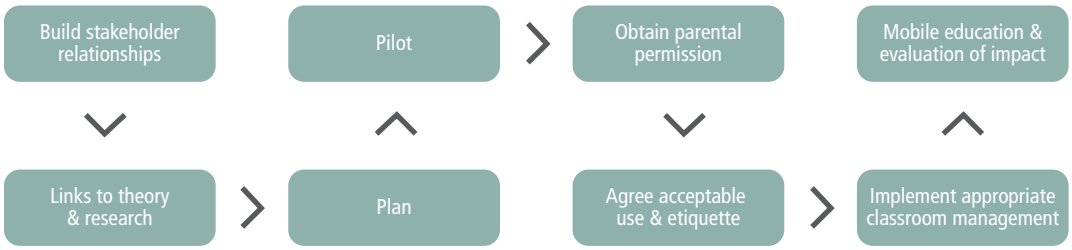
- Building relationships with all stakeholders (teachers, students, parents and guardians, school administrators, district authorities)
- Providing evidence that the use of mobile technology proposed is aligned to teaching and learning theory, research and national standards
- Planning of how the technology will be used including detailed lesson plans
- Proposing a pilot programme, including a detailed plan for how this would work, advice to "film videos of what you and your students are doing" and "publish on online spaces to celebrate the work your students are doing" and the suggestion to invite administrators to observe or even participate in some lessons
- Obtaining parental permission, establishing acceptable use policies and phone use etiquette and putting in place appropriate classroom management procedures

This process has been summarised and vital steps of evaluating the impact of the new approach added, in Figure 3.

47 Christensen C M, "The Innovator's Dilemma: The Revolutionary Book that Will Change the Way You Do Business, Collins 1997, ISBN-10: 0060521996

48 Engel, G et al, 2010, "10 Proven Strategies to Break the Ban and Build Opportunities for Student Learning with Cell Phones", The Innovative Educator, http://theinnovativeeducator.blogspot.com/2010/11/ten-building-blocks-to-break-ban-and.html

Figure 3: A Planned Approach to Introducing Mobile Technologies into the Classroom



Source: GSMA (based on Engel G et al)

2.4 Risk of students getting into financial difficulty

Most relevant to: all, but especially younger and more vulnerable learners

Solution type (policy, technical, culture change or staff development): technical, policy, staff development and learner guidance

Criticality: "*Potential to Discourage/restrict use*"

Description and discussion

If students are using their own mobile devices for learning, institutions will wish to be confident that there is no risk of them getting into financial difficulties as a result of incurring additional charges e.g. as a result of exceeding "fair use" data limits or due to roaming charges if using their devices in other countries.

Some projects, e.g. the Learning 2 Go project in the UK, have ensured there can be no problems by negotiating with mobile network operators fixed price "no surprises" contracts.

2.5 Risk of students getting into trouble due to illegal file sharing/downloading

Most relevant to: all, but especially younger learners

Solution type (policy, technical, culture change or staff development): technical, policy, staff development and learner guidance

Criticality: "*Potential to discourage/restrict use*"

Description and discussion

Institutions routinely implement measures to prevent students from accessing illegal file sharing and downloading websites when they are using desktop computers on their networks. Similarly, they need to consider what technical and educational measures are required to control this risk when mobile technologies are used, whether these are owned by students or the institution.

3. Health and Safety

3.1 Mobile phones and wireless networks alleged health risks

Most relevant to: all, but particularly children under 16

Solution type (policy, technical, culture change or staff development): if risk was ever established for either mobile phones or wireless networks it would lead to changed policies on use; technical changes; staff development

Criticality: Would significantly "*Discourage/restrict use*" if health risks were ever established. In some cases concerns about this currently "*discourage/ restrict use*" for some young learners and of WiFi in some schools. A "*minor or occasionally raised*" issue where educators are aware that most of their learners already own and use mobile phones and have WiFi in their homes.

Description and discussion

In most developed countries governments have funded research relating to possible health risks from mobile phones and networks. Most governments and the WHO have concluded that present human exposure recommendations are protective of all persons and that no specific measures are warranted for children.

The Health Council of the Netherlands[49] published a report in October 2011 that reviewed whether radio signals could affect the brains of children and concluded:

"*There is no scientific evidence for a negative influence of exposure to electromagnetic field of mobile telephones, base station antennas or Wi-Fi equipment on the development and functioning of the brain and on health in children.*"

The Health Council recommended further research, in particular into effects in young children and into long term effects but saw no reason to modify the current exposure limits, which have been designed with a large uncertainty margin especially to take into account possible vulnerable groups including children.

In May 2011 31 scientists from 14 countries evaluated all available research evidence for the WHO agency IARC[50]. They concluded there was 'limited evidence of carcinogenicity' for two types of cancer (where 'limited' means a causal interpretation is considered credible, but chance, bias or confounding could not be ruled out with reasonable confidence) and 'inadequate evidence' to allow conclusions about other cancers. As a result WHO/IARC has classified radiofrequency electromagnetic fields associated with wireless phone use as "possibly carcinogenic to humans (Group 2B[51])". Dr Jonathan Samet (University of Southern California), overall Working Group Chairman, stated "The conclusion means that there could be some risk, and therefore we need to keep a close watch for a link between cell phones and cancer risk[52]."

Due to uncertainty, in some cases governments have adopted precautionary measures including recommendations to limit use of mobile phones by children.

49 http://www.gezondheidsraad.nl/en/publications/influence-radiofrequency-telecommunication-signals-children-s-brains

50 International Agency for Research on Cancer, http://www.iarc.fr/

51 See http://monographs.iarc.fr/ENG/Classification/index.php for an explanation of the classifications and a list of classified agents

52 http://www.iarc.fr/en/media-centre/pr/2011/pdfs/pr208_E.pdf

Health research has also considered the potential risks of wireless networks. In Canada and France there have been concerns about the use of WLAN resulting in removal from a small number of schools.

The UK Health Protection Agency issued a statement regarding wireless networks in 2007: "*There is no scientific evidence to date that WiFi and WLANs adversely affect the health of the general population. The signals are very low power, typically 0.1 watt (100 milliwatts) in both the computer and the router (access point) and the results so far show exposures are well within ICNIRP[53] guidelines. Given this, there is no particular reason why schools and others should not continue to use WiFi or other wireless networks. However there has not been extensive research into what people's exposures actually are to this new technology and that is why we are initiating this new programme of research and analyses. We have good scientific reasons to expect the results to be re-assuring and we will publish our findings.*"
(Professor Pat Troop, Chief Executive of the Health Protection Agency).

The findings were published as Peyman, A, et al (2011)[54] and reported that "*The data gathered during the project continue to reinforce the position adopted by the HPA at the beginning of the project that exposures are small in relation to the ICNIRP guidelines and less than those from mobile phones. The outcome of the project will also be considered by the Advisory Group on Non-Ionising Radiation in its current health risk review of exposures to radiofrequency fields, which is expected to be completed in 2012.*"

This continues to be an active research field with new papers being published regularly. GSMA and the Mobile Manufacturers Forum (MMF) jointly prepare a monthly newsletter Mobile Abstracts[55] which provides a brief update of recent scientific publications related to mobile telephony.

Sources of information and advice

GSMA Mobile and Health information:[56] GSMA recognises that there is public concern about the siting of antennas and the use of mobile devices. These are low powered radio services and it is GSMA's opinion based on expert scientific reviews that there are no established health risks from exposures to radio frequency signals from mobile phones or wireless networks to the levels recommended by the WHO[57].

UK

- **Health Protection Agency**[58]
- **World Health Organization International EMF Project**[59]

3.2 Risk of mobile learners being targeted by thieves

Most relevant to: under 16s, vulnerable adults

Solution type (policy, technical, culture change or staff development): organisational policy, staff development and advice and guidance for at risk learners.

Criticality: May "*discourage/restrict use*" where teachers are concerned, in particular in the case of very young or vulnerable learners. A "*minor or occasionally raised*" issue where educators are aware that most of their learners already own and use mobile phones.

53 International Commission on Non-Ionizing Radiation Protection, http://www.icnirp.org/

54 Peyman, A, et al, 2011, "Assessment of exposure to electromagnetic fields from wireless computer networks (Wi-Fi) in schools; results of laboratory measurements" in Health Physics, 100, Issue 6, 594-612 see: http://journals.lww.com/health-

55 http://www.gsma.com/Mobile-Abstracts/

56 http://www.gsma.com/mobile-and-health/

57 http://www.who.int/peh-emf/en/

58 www.hpa.org.uk

59 www.who.int/emf

Description and discussion

Teaching and caring staff in educational institutions sometimes express concerns about giving young or vulnerable learners attractive and expensive portable technologies which could potentially attract the attention of thieves and therefore expose learners, for whom the institution has a duty of care, to danger.

Staff development around this issue focuses on awareness of the problem, how to advise learners and also the need for a proportional response based on the extent to which the risks these learners routinely face are increased, bearing in mind that the majority of young people in developed countries carry their own mobile devices.

Some projects (e.g. Wolverhampton local authorities in the UK) have sought to reduce the risk of theft by marking devices with large and recognisable project or organisation logos and by liaising with local police in developing advice.

3.3 Eye strain and RSI risks

Most relevant to: all

Solution type (policy, technical, culture change or staff development): organisational policy, staff development and advice and guidance for learners.

Criticality: "*minor or occasionally raised*" issue

Description and discussion

These health risks are only very occasionally mentioned as possible problems and relate to any use of mobile devices whether for education or other purposes.

GSMA provides the following information on this topic:

Repetitive Strain Injury (RSI) is used as an umbrella term to refer to various kinds of injuries to muscles, tendons or nerves caused by repetitive movement of a part of the body. It has not been medically established that texting and playing games on a mobile phone can cause RSI. If you are concerned, we recommend that when using a mobile phone for texting or playing games:

- Do not grip the phone tightly
- Press the buttons lightly
- Try to use both hands to spread the load
- Keep your hands close to your body when holding the phone
- Hold the phone up in front of you to reduce flexing of the neck
- Make use of the special features in the handset which minimise the number of buttons which have to be pressed, such as message templates and predictive text
- Take lots of breaks to stretch and relax

If you experience symptoms such as persistent or recurring discomfort, pain, throbbing, aching, tingling, numbness, burning sensation, stiffness, promptly see a qualified health professional. In the UK further information on RSI is available from NHS Direct[60] and the UK Chartered Society of Physiotherapy[61] has issued tips for people texting or playing games.

60 http://www.nhsdirect.nhs.uk/

61 http://www.csp.org.uk/

3.4 Sleep Disruption

Most relevant to: under 16s and vulnerable adults.

Solution type (policy, technical, culture change or staff development): staff development and advice and guidance for learners and parents.

Criticality: "*minor or occasionally raised*" issue

Description and discussion

The concern is occasionally mentioned that young people may sleep with their phones nearby resulting in interrupted sleep when they respond to calls or SMS. This is a possible problem and relates to any use of mobile devices whether for education or other purposes.

The findings of research into the impact of digital technologies on human wellbeing carried for the Nominet Trust[62] by neuroscientist Dr Paul Howard-Jones included the suggestion that: "how and when technology is used does appear to influence sleep. In particular, late night technology use is linked to reduction in sleep and sleep quality, and teenagers who use their mobile phones after "lights out" are considerably more likely to suffer daytime sleepiness."[63]

Dr Howard-Jones recommends: "Since many of today's parents did not grow up in a world that was as technologically rich as their children, they may not feel adequately prepared to provide the guidance that their children need. It may fall to another party such as schools, therefore, to provide the information required for parents and children. Indeed, pupils would benefit from schools delivering skills that support the 'hygienic' use of internet and digital technology (ie use that contributes to wellbeing, healthy development and effective learning).

3.5 Obsessive Use

Most relevant to: under 16s, under 25s, vulnerable adults, with some implications for others.

Solution type (policy, technical, culture change or staff development): staff development and advice and guidance for learners and parents.

Criticality: "*minor or occasionally raised*" issue

Description and discussion

The concern is occasionally mentioned that some young people may develop problems as a result of excessive use of technology. It has been observed that "There is a small sub-set of the population who find it hard to control how much time they spend online, to the point it interferes with their daily activities"[64].

This is a potential problem which is more likely to be noticed in the home than in an educational institution however it may arise as an issue in schools, colleges or universities and particularly in those that provide residential accommodation.

Sources of information and advice

Vodafone have produced a comprehensive Digital Parenting magazine[65] which provides advice on this and many other issues related to young people's use of technology. A dedicated section[66] of their website also provides specific information about excessive use and links to sources to further information and advice.

62 http://www.nominettrust.org.uk/

63 Howard-Jones, P, 2011, "The impact of digital technologies on human wellbeing", Nominet Trust, http://www.nominettrust.org.uk/knowledge-centre/articles/impact-digital-technologies-human-wellbeing

64 http://www.leeds.ac.uk/news/article/707/excessive_internet_use_is_linked_to_depression

65 http://www.csp.org.uk/

66 http://parents.vodafone.com/

4. Learner Privacy and Autonomy

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical, culture and staff training

Criticality: "*Potential to discourage/restrict use*"

Description and discussion

Mobile technologies provide opportunities for monitoring and protecting learners which would previously have been either impossible or impractical. Well documented risks relating to internet content and communication as well as the portability and value of mobile technologies encourage the development of well-meaning strategies and tools to monitor and protect both learners and the technologies they carry. However these may sometimes be considered excessive and an invasion of privacy by the learners who are being protected.

Some institutions have even started to use systems that monitor online postings by their students in order to detect cyber-bullying[67].

It is necessary for institutions and societies to debate what monitoring and protection is acceptable to both individuals and the society they live in and what the impact is on the autonomy and freedom of young people. There is clearly a delicate balance to be achieved which provides adequate but not excessive or unacceptable protection.

For example, institutions may wish to:

- **Track the physical location of learners or devices** e.g. if students are using mobile devices on a school trip schools might wish to use tracking in case the students or the devices get lost. All but the youngest learners are likely to consider continuous automatic tracking of their location unacceptable. If older students are aware that their mobile devices are being tracked they may worry that their location is also being tracked. However when a device is lost or stolen the user may be assisted by a system which can locate and/or disable it (see section 5.3 "Protection of data on mobile technologies" and section 6 "Mobile device management")
- **Monitor learners browsing or communication**. Most learners would consider monitoring of their phone calls, texts or communication via social networking sites a serious invasion of privacy. However many may accept as not unusual that their school/college/university will keep some record of the websites they visit via institutional networks and equipment. If institutions are doing this, the policy should be transparent including making clear to students that the institution has access to their browsing history when they are using devices or networks supplied by the institution.

Consideration of learner privacy is also necessary when educational institutions communicate with learners via their personal mobile devices. For example too frequent messaging may be perceived as spam and therefore impacting on privacy. Personal mobile numbers are considered private and should be used only in the context of learning services provided by the institution. Institutions should have internal acceptable use policies (see section 7) that identify appropriate and inappropriate use of information about the private devices and data of students. Such policies should reflect local law or guidelines.

67 See e.g. http://www.smh.com.au/technology/technology-news/schools-use-the-net-to-eavesdrop-on-students-20110812-1iqx2.html

A potential future use of students' mobile technologies is to authenticate their identity for purposes such as entry into buildings or labs, access to physical resources, cashless payment in cafeterias or for photocopying, etc. Currently institutions commonly use cards for these activities and transactions. In some cases students' finger or thumb prints are used which can be the source of some privacy questions and concerns. All of these introduce unique privacy questions and concerns which will need to be addressed on a case by case basis.

Sources of information and advice

Research carried out for GSMA has explored mobile users' attitudes and perceptions regarding privacy (Futuresight, 2011[68]).

GSMA has developed a voluntary Mobile Spam Code of Practice for mobile operators[69] that applies to unsolicited SMS and MMS messages. Some of the provisions of the Code of Practice could also inform development of institutional policies on messaging.

JISC, the UK's expert agency for information and digital technologies for education and research, provide detailed advice regarding student privacy[70]. They have also published an online mobile learning information kit[71].

68 Futuresight, 2011, "User perspectives on mobile privacy, Summary of research findings", http://www.gsma.com/mobile-and-privacy-resources/

69 http://www.gsma.com/documents/mobile-spam-code-of-practice/20043

70 http://www.jisc.ac.uk/supportingyourinstitution/studentjourney/mobilelearning.aspx

71 https://mobilelearninginfokit.pbworks.com/w/page/41753164/Overview

5. Data and Systems Privacy and Security

All online systems require effective access controls and efficient management of data including arrangements for storage, backup, access control, editing permissions, copying and downloading controls and prevention of interception or corruption during transmission. Some of these arrangements are more complex when: the users of the data are mobile, the technology is very easily portable and when access is via wireless and mobile networks.

In the context of mobile education, privacy is particularly important for sensitive data such as learners' personal details and communications, confidential information about learners, assessment data, confidential institutional data and data confidential to the employers of workbased trainees and professional learners. Handling of such data is subject to the provisions of existing data protection, e-privacy and interception legislation e.g. in the UK the Data Protection Act 1998, the Privacy and Electronic Communications Regulations and the Regulation of Investigatory Powers Act.

JISC, the UK's expert agency for information and digital technologies for education and research, provide detailed advice related to Data Protection legislation requirements and make broader recommendations concerning best practice in data privacy and security.

They recommend that:

"Institutions considering adopting new administrative systems and other processes with possible privacy implications, or updating existing systems or processes (such as student record systems, virtual learning environments (VLEs), ePortfolio systems and distance learning programmes) should consider undertaking a Privacy Impact Assessment (PIA) in the early stages of project or process design, well before roll-out/ implementation. Privacy Impact Assessment can be defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a constructive search is undertaken for ways to avoid, minimise or at least ameliorate privacy concerns"[72].

GSMA's Mobile Privacy Initiative has been working with its members, and engaging with other players in the broader ICT ecosystem, to consider the privacy challenges in the mobile sector. The Mobile Privacy Principles[73] published by GSMA in January 2011 describes the ways in which mobile consumers' privacy should be respected and protected.

The principles apply to applications and services that may impact a user's privacy. This includes applications or services that seek to access, collect and otherwise use personal information and other private data about users which may be held on a mobile handset or which information may be generated by the end users use of a mobile application or service. They also apply to activities that impact user privacy in other ways, such as through intrusion, unwarranted contact or real–time monitoring.

The GSMA has also developed, and invited comments on, a set of Privacy Design Guidelines for Mobile Application Development[74] (and an annex of illustrative examples[75]). These guidelines seek to articulate the Mobile Privacy Principles in more functional terms and are intended to help drive a more consistent approach to user privacy across mobile platforms, applications and devices.

72 Charlesworth A, Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998, JISC Legal, 2009

73 http://www.gsma.com/mobile-privacy-principles/

74 http://www.gsma.com/mobile-privacy-design-guidelines/

75 http://www.gsma.com/documents/annex-of-illustrative-examples-pdf-577-kb-16-pages/20009/

GSMA Mobile Privacy Principles defines 'personal information' which should be safeguarded as including (but not limited to) the following types of information that relate to "a mobile user and their use of mobile applications and services and information which may be considered private by users even though it may not be strictly protected in law:

- Any data that is collected directly from a user (e.g. entered by the user via an application's user interface and which may include name and address, credit card details)
- Any data about a user that is gathered indirectly (e.g. mobile phone number, email address, name, gender, birth data, location data, IP address, IMEI, unique phone ID)
- Any data about a user's behaviour (e.g. location data, service and product use data, website visits)
- Any user-generated data held on a user's device (call logs, messages, user-generated images, contact lists or address books, notes, and security credentials)

5.1 Protection of data on institutional servers

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical,

Criticality: "*Potential showstopper*" if not adequately addressed

Description and discussion

Data on institutional servers is protected by access controls, firewalls, anti-virus and anti-malware software. With the increasing use of mobile technologies by learners institutions have become increasingly concerned about the risk of learners introducing viruses, accessing systems and data they should not have access to, unauthorised downloading and heavy usage degrading network performance.

Many institutions have responded to these risks by implementing separate wireless networks for learners, and visitors, to access the internet from their mobile devices whilst allowing no access to institutional systems and databases. Other institutions have implemented mobile device management (MDM) systems which enable more sophisticated control and assist with the administrative workload resulting from opening up access from many and varied devices. See section 6.2 for more information about MDM systems.

5.2 Protection of data in cloud services

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical,

Criticality: "*Potential showstopper*" if not adequately addressed

Description and discussion

Many educational institutions are exploring the possibilities of, or already using some, "cloud" computing services. These services are attractive due to ease of access from many locations and their cost efficiency and scalability as institutions buy an externally managed service paying according to the required storage, functionality, traffic and bandwidth instead of needing to purchase, maintain and support locally the servers and software used.

However some managers, teachers and learners may worry that externally stored private data might be less secure than that held on institutional servers and these worries have not been allayed by the much publicised Sony PlayStation Network security breach in which millions of customers' personal details were stolen. In reporting this incident Reuters[76] quoted Gartner's cloud security analyst Jay Heiser's advice "If you're doing anything that is critical to your business [using cloud services], you need contingency plans".

An additional concern for mobile education is that access to data in cloud services is dependent upon online connectivity. This can be disrupted when learners move into areas without coverage, or with reduced signal strength, or if signal is interrupted.

Services may also be disrupted by problems occurring at the providers' data centres. An Amazon Web Services incident in which cloud based services were disrupted for several days led to some analysts to question whether cloud computing is a good idea, although others have suggested that "cloud computing in fact will emerge much stronger for the experience" (Chandras, R, 2011[77])

Many teachers have, perhaps without realising, used cloud computing services because they have used free services such as Dropbox to store materials online for their learners to access from any computer or internet enabled mobile device. These teachers have found such services to be very useful and very easy to use. However, although providers of these services do use encryption to protect data, some security experts have warned that it is not necessarily infallible and offer advice such as "though it's a cool tool, don't store anything that's super-sensitive on it." (Feldman, J, 2011[78]). Also, the use of such services and the storage of student data must be done in ways that ensure compliance with data protection and privacy laws.

5.3 Protection of data on mobile technologies

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical,

Criticality: "*Potential showstopper*" if not adequately addressed

Description and discussion

A number of high profile news reports about laptops containing sensitive data being left on public transport, in taxis or otherwise mislaid and mobile devices being "hacked", have raised awareness of risks to data on mobile devices.

In education this data might relate to:

- the user of the device, e.g. personal communications, personal data or data about their progress and assessments
- an employer of the learner e.g. commercially sensitive data
- clients of the learner's employer e.g. in medical education, sensitive data about patients and their care

76 Finkle, J & Baker, L, 2011, "Sony woes may cause some to rethink cloud computing", Reuters, http://uk.reuters.com/article/2011/05/09/uk-sony-cloud-idUKLNE74803820110509?feedType=RSS&feedName=everything&virtualBrandChannel=11708

77 Chandras R, 2011, "Wake-Up Call For Cloud Vendors And Customers", Information Week, http://www.informationweek.com/news/cloud-computing/infrastructure/229503443?queryText=%26quot%3B2011+Strategic+Security+Survey+%26quot%3B

78 Feldman, J, 2011, "Global CIO: The Dropbox Deception: Caveat Emptor", Information Week, http://www.informationweek.com/news/global-cio/interviews/229502488?queryText=%26quot%3B2011+Strategic+Security+Survey+%26quot%3B

JISC Legal advise UK universities and colleges that:

"Employees and students should take particular care when laptop computers or personal machines are used to process institutional personal data at home or in other locations (e.g. in public places, or on public transport) outside the institution. Laptops containing personal data should have properly implemented security measures that are proportionate to the anticipated risks and appropriate to the type of personal data to be transferred. These may include passwords, biometric security mechanisms and encryption. The increasing capacity and declining size of storage media, such as CDs, mini hard disk drives, and USB flash memory data sticks means that it is possible for employees and students to carry considerable amounts of personal data on media that are easily lost or forgotten. Institutions should consider the provision of advice to employees and students about the appropriate use of such media and the need for adequate security measures to reduce data breaches in the event of loss or theft."[79]

When sensitive information may be stored on mobile technologies, and when they are used to access online information, 'common sense' precautions should be used e.g. setting up an access password which cannot be easily guessed.

Where there is particular concern about privacy of data on the device it may be possible to arrange that data will be erased after 10 failed password attempts. Other precautions the end user of the device can take include not clicking on adverts and pop-ups, not responding to unsolicited emails and not storing private or very personal information on a mobile device, especially PINs and passwords.

MDM systems or Apps such as "find my iPhone" can be used to locate, lock and wipe all data stored on lost or stolen devices. This type of protection is not infallible but will protect against most casual thieves who are interested in the device rather than the data on it.

Perhaps surprisingly, many commercial companies, whose data and contacts on mobile devices are more likely to be commercially valuable or sensitive, have not implemented MDM systems. Research by Information Week (Davis, M, 2011[80]) found that only 33% of 1,084 corporate respondents "use mobile device management (MDM) software to enforce a unified security policy".

MDM systems are starting to be used by large educational institutions, with the motivation often being to assist with IT support workload and to control support costs.

GSMA maintains the IMEI Database (IMEI DB). The IMEI DB is a global central database containing basic information on serial number (IMEI) ranges of millions of GSM and 3G devices (e.g. mobile phones, laptop data cards) that are in use across the world's GSM networks. The IMEI is a 15-digit number that is used to identify the device when it is used on a GSM mobile phone network. The IMEI DB also supports a "black list" of IMEIs that are associated with GSM or 3G devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. The IMEI DB acts as a central system for network operators to share their individual black lists so that devices denied service (blacklisted) by one network will not work on other networks even if the SIM card in the device is changed.

GSMA advice concerning risks from viruses and other malicious software notes that there is much less mobile phone malware in existence than computer malware and current mobile phone malware is less sophisticated and poses significantly lower risk than computer malware. However it is possible that mobile phone malware will become more common in the future.

79 Charlesworth A, 2009, "Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998", JISC Legal

80 Davis, M, "2001 Strategic Security Survey", Information Week Analytics, May 2011, Report ID: R2130511, http://www.clearnorthtech.com/images/research-2011-strategic-security-survey_336711.pdf

GSMA advise that it is prudent for mobile phone users to take some precautions.

For example:

- Never install any software onto your mobile phone unless you know and trust the source of that software and you were expecting to receive it
- Never ignore or override security prompts displayed by your phone unless you are confident that you fully understand the risks
- Never load unauthorised ('pirate') copies of software onto your phone as these may be carrying hidden viruses or other malicious code
- If you are particularly concerned consider installing specialist anti-virus software. For more advice: Computer Viruses and Mobile Phones[81]

When installing anti-virus software on mobile devices it is important that institutions, teachers and students are aware that there may be a risk that this could be circumvented when bluetooth is used to enable a mobile phone to act as a modem for a laptop. Within a topic of "Laptop and Mobile Device Security" the Dummies.com website includes the warning "most device-based firewalls typically cover all IP interfaces - WLAN, GPRS/EDGE, 3G, LTE, and the like - and they may not provide specific coverage for the Bluetooth interface" (Campagna, R et al, 2011[82]).

A potential risk to data stored on mobiles, dubbed juicejacking[83], has been identified related to the use of public charging stations using USB connections which in some cases could be used to access data as well as provide power. The easiest ways of avoiding this risk are to use the charging adaptor supplied with the mobile device or to purchase a battery-powered recharger.

Sources of information and advice

GSMA Security advice[84] for mobile phone users, includes advice related to preventing mobile phone theft, spam and mobile phones and secure use of voicemail services.

5.4 Protection of data during transmission

Most relevant to: all

Solution type (policy, technical, culture change or staff development): technical

Criticality: "*Potential showstopper*" if not adequately addressed

Description and discussion

Educational institutions might have concerns about the security of data and communication during transmission to and from mobile devices.

Mobile operators use GSM security algorithms to provide authentication and radio link privacy to users on a GSM network. GSM uses three different security algorithms called A3, A5, and A8. In practice, A3 and A8 are generally implemented together (known as A3/A8).

81 http://www.gsma.com/viruses-and-mobile-phones/

82 Campagna, R et al, 2011, "Enterprise Mobile Device Bluetooth Security Issues", Dummies.com,http://www.dummies.com/how-to/content/enterprise-mobile-device-bluetooth-security-issues.html

83 http://nakedsecurity.sophos.com/2011/08/19/is-juicejacking-the-new-firesheep/

84 http://www.gsma.com/security-advice-for-mobile-phone-users/

An A3/A8 algorithm is implemented in SIM cards and in GSM Network Authentication Centres. It is used to authenticate the customer and generate a key for encrypting voice and data traffic. An A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy. An A5 algorithm is implemented in both the handset and the base station subsystem (BSS).

The use of mobiles with wireless networks can pose some security risks if action is not taken to make these networks secure. Educational institutions' IT departments are aware of this and therefore official WiFi within institutional premises is likely to be secure.

However risk can be introduced if students connect to unsecured WiFi at home or in the community or if staff set up local or temporary WiFi without implementing appropriate security measures. Such Wifi could be misused by unauthorised users for illegal activities or to access inappropriate material. In some countries, e.g. Germany, people must secure their wireless connections to prevent others from illegally downloading data and can be fined if a third party takes advantage of their unprotected line, although they are not held responsible for illegal downloading by the third party. Connecting via mobiles to unsecured wireless networks can also increase the risk of hacking thereby putting personal data at risk.

Educators and students should also be made aware of the potential risk of connecting, deliberately or automatically, to bogus WiFi gateways which criminals may have set up in public places in order to collect personal data, particularly credit card details[85].

Sources of information and advice

- GSMA security algorithms information[86]
- Wireless Broadband Alliance[87]

5.5 Mobile learning content management

5.5.5 Content storage, searching, sharing and editing

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical, culture and staff training

Criticality: "*Potential to discourage/restrict use*" if not adequately addressed

Description and discussion

Educational content management is commonly arranged by the use of Managed Learning Environments (MLEs)/Virtual Learning Environments (VLEs)/Learning Management Systems (LMS). Learning materials and resources are often stored in content repositories or accessed via systems and portals that facilitate educational content sharing. MLE/VLE/LMS systems safely store and control access to educational materials.

Some educational materials, especially "bite sized" content commonly used in mobile education may reside in folders on institutional servers and be distributed to learners' mobiles via email or SMS.

Also, increasingly, mobile learning materials are externally hosted or obtained - e.g. Apps downloaded from and updated via Apps stores, You Tube videos (either stand alone or within dedicated institutional channels), 3rd party pod and pod casts and material shared via web 2.0 services.

85 http://www.guardian.co.uk/technology/2011/apr/25/wifi-security-flaw-smartphones-risk

86 http://www.gsma.com/security-algorithms/

87 www.wballiance.net

Many materials and resources used for mobile teaching and learning are created by individual teachers, learners, experts and enthusiasts, whilst others may be purchased from specialist developers and publishers.

Educational content is sometimes pre-loaded on to students' mobile devices in order to guarantee fast access in locations and situations where mobile signals may be unavailable or interrupted and Wifi is unavailable or provides insufficient bandwidth for simultaneous usage by large groups.

5.5.6 Protection of institutional/academic IPR and Copyright

Most relevant to: all

Solution type (policy, technical, culture change or staff development): policy, technical, culture and staff training

Criticality: "*Potential to discourage/restrict use*" if not adequately addressed

Description and discussion

Where educational content is downloaded to learners' mobile technology measures may be required to protect the institution's copyright or IPR.

Existing laws on protection of 3rd party copyright and IPR apply where teaching and other educational institution staff are creating educational content. This legislation will be familiar to institutional management. However many teachers may not previously have given much consideration the implications of using and sharing multiple media – pictures, videos, drawings, audio – before starting to create learning materials and activities for mobile devices. Therefore staff training should be in place to ensure compliance with the law and avoidance of financial and reputational penalties whilst continuing to encourage rather than stifle staff creativity.

6. Mobile device management

6.1 Multiple device delivery, storage and maintenance

Most relevant to: all institutions

Solution type (policy, technical, culture change or staff development): policy and technical

Criticality: "*Potential to discourage/restrict use*" if not adequately addressed

Description and discussion

Many mobile education projects involving providing learners with handheld devices have found that they initially underestimated the amount of work that would be generated for IT staff and/or project staff in getting mobile devices ready for issuing to learners e.g. taking delivery of large numbers of devices; unwrapping, charging; installing SIMs; installing software; device configuration and creating and copying a standard image.

The MoLeNET Learning2Go Further project evaluation reported as a valuable contribution the mobile operator partner (O2) taking on responsibility for "*…pre-imaging of the devices, the packaging of e-safety information in the boxes and the establishment of a delivery process which enabled the safe delivery and hand over of devices*".

Security issues at this time include ensuring safe storage of devices, asset tagging and perhaps marking with institution or project logos to make them less likely to be stolen.

Privacy issues arise as it often helps overstretched small IT departments as well as teachers if teaching and other appropriately trained staff are given access rights which allow them to control tasks like downloading or updating software on devices.

6.2 Institutional mobile device management

Most relevant to: all institutions

Solution type (policy, technical, culture change or staff development): policy, technical and staff development

Criticality: "*Potential to discourage/restrict use*" if not adequately addressed

Description and discussion

The introduction of mobile education involves increased workload for IT departments who may for this reason seek to discourage it. A key lesson reported by many projects is the importance of involving the IT department at an early stage and obtaining their commitment and co-operation.

Commercial organisations which supply mobile technologies to large numbers of staff often use centralised Mobile Device Management (MDM) systems to assist support. Educational establishments are starting to use the same systems to help them to support mobile devices used by both staff and students.

MDM systems enable organisations' IT departments to:

- Locate, track and gather information on the movement of GPS enabled devices
- Be alerted to automatically monitored device and server system events
- Remotely diagnose and fix problems
- Deploy software, data and configuration details to devices in real-time over WiFi and mobile networks
- Remotely disable and wipe data from lost or stolen devices

MDM systems usually consist of a server component, which sends out management commands to the mobile devices, and a client component on the mobile device, which receives and implements the management commands. Organisations may buy both components from a single supplier or may purchase the server and client components from different sources.

Loss, theft or damage of institutional mobile devices

Very consistent messages have emerged from many projects in several countries over the last decade indicating that when young people, including and particularly disadvantaged or excluded young people, are trusted to look after new technology they take very good care of it.

Teachers and institutional managers have often had their initial fears proven groundless by experience in practice in both laptop and mobile education projects. For example the MoLeNET programme[88] involved 40,000 learners and the incidence of lost, damage and theft of mobile technologies during the 3 years of the programme was less than 1%.

6.3 Bring-your-own-device management

Most relevant to: all institutions

Solution type (policy, technical, culture change or staff development): policy, technical and staff development

Criticality: "*Potential to discourage/restrict use*" if not adequately addressed

Description and discussion

The introduction of BYOD or BYOT (Bring Your Own Technology) arrangements is an emerging trend in mobile education where institutions allow, enable, and in some cases encourage or require, learners to bring their own mobile devices to use in their education.

88 www.molenet.org.uk

There are a number of advantages to this approach, including:

- Providing a more flexible service in response to learner demand and thus improving learner satisfaction
- Learners are not inconvenienced by a requirement to carry extra mobile technologies in addition to their personal devices
- Learners pay for the devices (institutions may subsidise or arrange instalment payments)
- Learners tend to be motivated to replace and upgrade their mobile technologies more frequently than institutions
- The institution may be able to reduce its investment in fixed desktop computers and may be able to make more use of the rooms which housed these PCs

However there are a number of challenges and responsibilities implied including:

- Ensuring there is no interference with learners' personal software, apps, configuration and data resident on their device
- Respecting learners ownership of the device and their online and mobile space
- Avoiding excessive mobile communication which might be perceived as spam by learners
- Increased IT support workload and complexity as learners seek assistance or advice on a wide variety of device types and models
- Arranging appropriate access to institutional resources and preventing unauthorised downloading
- Virus and malware control
- Ensuring availability for sufficient electric sockets/charging stations for learners to charge personal mobiles

One expert, writing for a corporate IT audience, has warned that BYOD can translate to "bring your own disaster" if appropriate mobile device management policies and MDM systems are not implemented (Finneran, M, 2011[89])

It has been observed that in some cases implementing a single MDM system may not be sufficient. Changes occurring in many commercial companies as a result of BYOD have been described as: "*IT departments need to make a significant investment to support a diverse range of mobile devices and operating systems. Typically, with a homogenous fleet of devices, IT managers would have access to a device management suite enabling them to set standard security and access protocols across individual devices. Yet, these proprietary systems only support one type of device or operating system. IT managers are faced with having to deploy multiple device management systems each separate to the other and each with their own functionality, usability and protocols. Things are about to get a lot more costly and challenging.*" (Steger, H, 2010)[90]

Steger suggests one solution to this problem may be implementation of open source cloud-based device management solutions to "*provide the glue that stitches disparate devices and platforms together*". He also suggests that mobile operators could offer cloud based systems to help organisations manage large heterogeneous collections of mobile technologies as such systems "*have already been deployed by mobile operators globally, who by their very nature, face the same fragmentation issue across their networks but on a much larger scale.*"

89 Finneran, M, "BYOD Requires Mobile Device Management - To keep "BYOD" from translating to "bring your own disaster," IT needs MDM", Information Week, May 07, 2011 12:00 AM

90 Steger, H, "Magic Pads", IT Now, July 2011, BCS

7. Development and implementation of policies and acceptable use agreements

In both the commercial world and educational institutions safeguarding, privacy and security policies for regulating staff and student use of IT systems and data have traditionally been developed by IT departments. A typical IT policy lifecycle (e.g. as defined by Campagna, R et al, 2011[91]) involves the IT department defining the policy, communicating it clearly to system users, implementing the policy, auditing to assess whether the policy objectives are being met and over time making modifications in response to audit results and feedback.

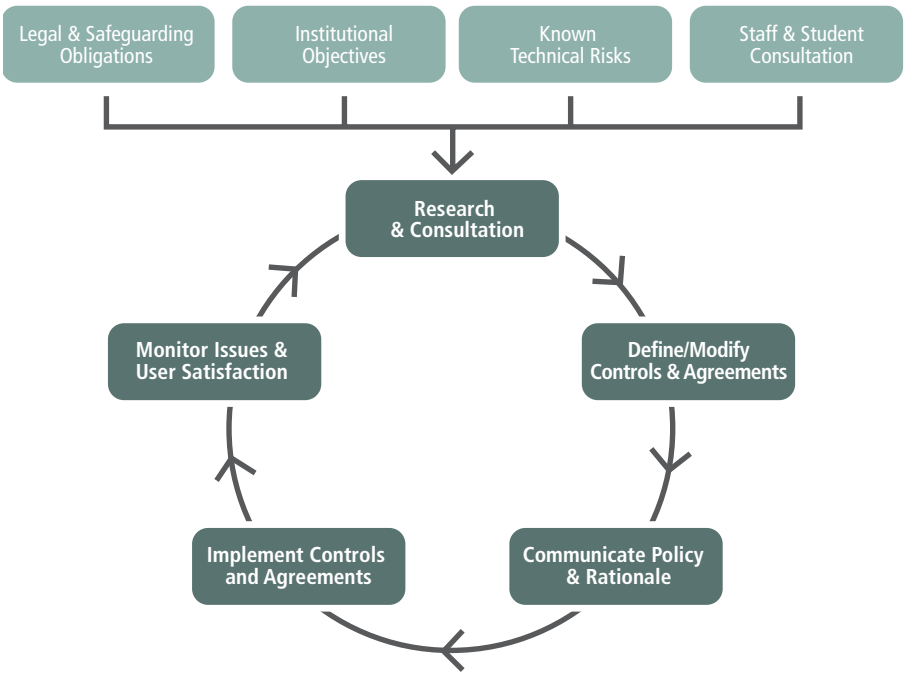
However staff and students are increasingly expecting to have the freedom to access and share information from a huge variety of sources both internal and external, are used to being able to use social networking systems for both social and educational purposes and may be doing this via their own technologies with or without institutional approval.

Also with increased use of mobile technologies for learning, and to communicate with learners, there is a need for acceptable use policies to extend to consideration of what is acceptable behaviour on the part of the institution, for example when it is or is not acceptable to send text messages to learners mobile phone numbers.

Therefore some institutions have decided to consult students, and their teachers or tutors, in the initial stages of defining policies and acceptable use agreements as well as seeking their feedback on implemented policies. The resulting policy cycle is illustrated in Figure 4.

Institutions have found that students are more likely to understand, respect and adhere to policies and acceptable use agreements that they have helped to develop.

Figure 4: Policy Development Cycle for the use of Mobile Technologies in Education



Source: GSMA 2012

91 Campagna, R, Iyer, S & Krishnan, A, "The importance of enforceable mobile device security policies", http://www.dummies.com/how-to/content/the-importance-of-enforceable-mobile-device-securi.html

8. Conclusions

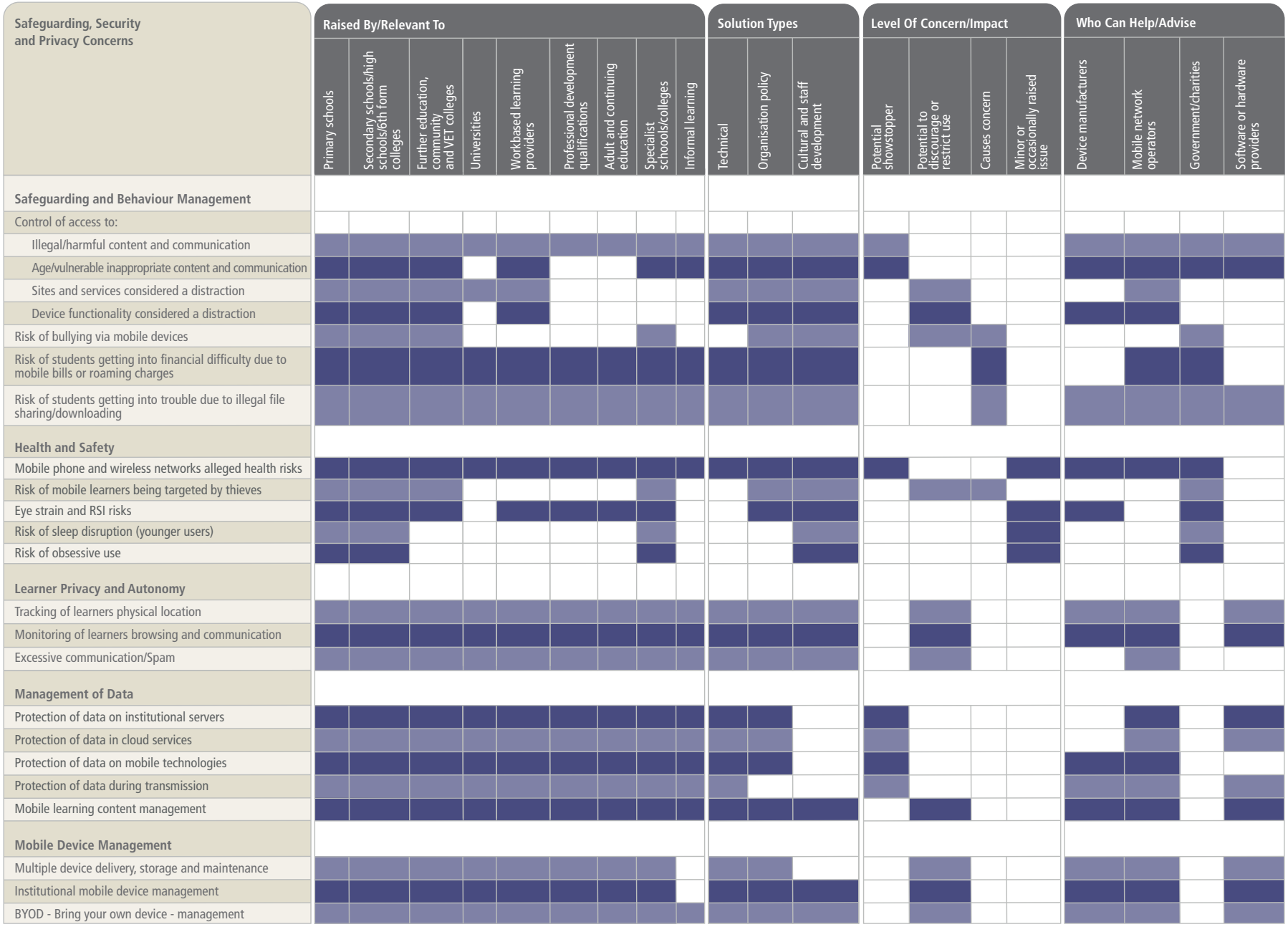
Educators may have a number of concerns which can act as a barrier to the introduction of mobile technologies to deliver or support teaching and learning or which can reduce the benefits accruing from the use of these technologies.

However information, advice and assistance available from a variety of sources can help to allay fears, address concerns and maximise the benefits enjoyed by both institutions and students.

Sources of advice and assistance include GSMA, government funded departments, centres and national support agencies, published mobile learning research, educators and institutions sharing their own experiences, device manufacturers, solutions providers and mobile network operators.

Appendix

Safeguarding, Security and Privacy Concerns Matrix



About GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and entertainment organisations. The GSMA also produces industry leading events such as the Mobile World Congress and Mobile Asia Expo.

GSMA's Mobile Education initiative aims to accelerate the adoption of mobile education solutions, particularly mobile-enabled portable devices, such as e-Readers and tablets, in mainstream education settings. This global initiative seeks to understand the landscape and address the barriers and opportunities in this emerging market.

GSMA Connected Living

GSMA Head Office
Seventh Floor, 5 New Street Square,
New Fetter Lane, London EC4A 3BF UK
Tel: +44 (0)207 356 0600
www.gsma.com
mhealth@gsm.org