Internet safety in schools

This essay addresses the topic of internet safety in terms of how it relates to school contexts. A focus is taken on compulsory education within the UK. The essay draws on governmental resources, and from work from charitable and educational sector organisations, in supporting online safety measures relevant to schools. The essay also discusses the implications of the 2018 GDPR (General Data Protection Regulations) in terms of their relevance for educational settings.

With the pace of developments in online technology, the relationship between the operation and administration of education and convergence culture bringing the online and the offline together in ever more-complex ways, and the increasing sophistication of the uses made of technology, it is imperative that schools keep abreast of current thinking regarding internet safety (Jenkins, 2008; Hunter, 2012). Statutory guidance from the UK government with respect to schools' safety is updated regularly; the next iteration of this guidance becomes effective September 2018, replacing the current 2016 version (Department for Education, 2018; Department for Education, 2016). The guidance – entitled Keeping Children Safe in Education – discusses recruitment checks, safeguarding protocols and how to work in instances where allegations are made; an annex to the document focuses on online safety (Department for Education, 2016). Here, the potential issues which face educationalists and learners alike are summarised: these range from online radicalisation, accessing illegal or pornographic material, child sexual exploitation and the activities of sexual predators, both within and outside the school (Department for Education, 2016).

The guidance document advocates a whole-school approach in terms of three main areas of risk and concern (Department for Education, 2016). First, that of content: "being exposed to illegal, inappropriate or harmful material [including] fake news, racist or radical and

extremist news" (Department for Education, 2018, p. 92). The second area is that of contact; this is outlined not only in terms of abusive or predatory behaviour by others, but also commercial advertising. The third area is conceived of as conduct-related: "personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying" (Department for Education, 2018, p. 92).

An ongoing requirement is for settings to limit pupils' access to potential risk via the school's computer system through the use of appropriate filtering software and oversight via monitoring systems; while there is latitude on the nature of the systems and policies put into place so that the school can contextualise their approach to local needs, there is an expectation that settings will articulate their online safety protocols with their Prevent duty risk assessment (Department for Education, 2018; HM Government, 2016). The Prevent duty, which explains public bodies' obligations under the Counter-Terrorism and Security Act 2015 to support prevention of people being drawn towards terrorism and other forms of extremist activity, states that such bodies are "expected to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (HM Government, 2016, p. 12; HM Government, 2015). Furthermore, this should be supported by staff training to support school staff in identifying such risks, challenging extremist thought, and making appropriate referrals where there are concerns to be addressed (HM Government, 2016).

Filtering software should be flexible to that it can be adjusted - for age groups or other forms of differentiation where appropriate - should be easily-controllable by staff, be backed by a clear policy, and be able to identify users. Such software should operate at a network level rather than at the level of the individual device being used, and should allow reporting where problematic sites or other issues are encountered so that both system usage and new sites

where there are concerns may be addressed (UK Safer Internet Centre, 2018). Furthermore, there should be an interlocking range of monitoring strategies in place. These include physical monitoring of learner online activity by staff, oversight of search terms and of sites accessed, with the capacity for internet access to be suspended immediately is an issue is encountered, and the issue of technological solutions which may, for instance, be keyword or keystroke-responsive (UK Safer Internet Centre, 2018).

Such initiatives should be contextualized to a whole-school approach which integrates positive messages about safe internet usage, the potential dangers of the internet, and clear mechanisms for pupils to voice their own concerns across the curriculum (HM Government, 2016; Rooney, 2014). Schools also need to consider their policies as regards pupils' personal access to the internet via their own mobile devices, as this will fall outside the boundaries of the school network (HM Government, 2016). The guidance documentation also offers links to education-sector agencies dealing with different aspects of online safety from purchasing of hardware and software, training packages, and on appropriate guidance on internet security protocols. While schools are encouraged to make their bespoke arrangements with respect to online safety, there are links offered to a range of organisations and charities with a remit which engages with key aspects of appropriate and safe online conduct, and its contextualisation to different curriculum areas (HM Government, 2016). Exemplar materials – including sample and customisable policies addressing online safety, acceptable use of school network facilities, and responding to an e-safety incident are available from children's charity the NSPCC; these include a self-assessment tool for schools so that an audit may be undertaken in respect of the comprehensiveness of setting policies and procedures (NSPCC, 2017). Local authorities my provide centralised support for schools who are grant-maintained, and there are multiple consultancies who can provide such support on a fee-paying basis. Furthermore, organisations such as the UK Council on Child Internet Safety

offer frameworks which support positivity in pupils' online engagements, from matters related to copyright to online information management which is graduated so that it can be mapped across to different Key Stage levels of national curriculum documentation (UK Council on Child Internet Safety, 2016).

There is, then, a significant amount of authoritative information, guidance and support available for schools to develop their own approach to internet safety, and to support pupils' own understanding (Stowell, 2016). As noted above, this is important not least because of statutory responsibilities with respect to the Prevent duty, but also because of the pace of change within relevant pedagogic technologies, and the legislation developed to engage with such advances (Ribble, 2015). An example of this is the 2018 GDPR data regulations, to which this essay now turns.

The GDPR regulations address the handling of personal data. Schools process an immense amount of such data in many different ways: enrolment and attendance records, medical information, job applications, software which supports homework completion payments for school meals are just a few examples of the ways in which personal data is collected and processed. The key shift in the new regulations – effective May 2018 – is a move from lawful holding and processing of such data to one where organisations need to be able to evidence compliance with data protection laws (Lock, 2018). Requirements for schools include: mapping computers systems' use of personal data and the ways in which legal compliance is satisfied; the appointment of a Data Protection Officer to oversee compliance; having agreements in place with third parties processing data on behalf of the setting which evidence GDPR compliance; training for all staff so that there is a cultural shift and personal ownership of the issues raised by the new regulations; and effective monitoring and reporting systems in case of a data breach (Lock, 2018). There also needs to be a publication scheme in

place so that it is clear what information is made available to the public (such as examination results) as well as guidance on related issues, such as how to approach the use of personal computing devices by staff to process personal data when, for example, marking from home (Information Commissioner's Office, 2018). The post of Data Protection Officer – which might be shared across sites for large academy organisations – is crucial, not least because the impacts of the new legislation are wide-ranging and there is a need for local expertise; however, the responsibilities for safe and compliant handling of personal data impact on all staff working within educational contexts (Information Commissioner's Office, 2018). The GDPR regulations offer a reminder that internet safety relates not only to the more obvious dangers of extreme content, of inappropriate material being accessed, or the potential for radicalisation, but also of informational security (Attai, 2018). The regulations also offer reminders to practitioners of the value of supporting learners to appreciate for themselves the value of their personal data, and to be proactive in their use of online resources in protecting their identity and other data resources accordingly across the curriculum (Lau, 2017).

This short essay has worked to discuss issues connected to internet safety in educational contexts in the UK. As the essay has shown, there is a mix of legal requirements and good practice standards for settings to engage with, and a proactive and setting-wide approach is only appropriate. The centrality of online engagement to contemporary education, and the importance of teaching and learning in ways which recognise both the opportunities and potential issues of online worlds, both mean that a cohesive, detailed and proactive approach which involves all operational and strategic aspects of the setting is appropriate. There is a spectrum of support available through relevant educational, charitable and governmental sources. However, the onus is on the setting to engage with these support mechanisms to not only ensure compliance and safety, but to be proactive so that staff and learners alike are

aware of potential dangers, but can still work and learn safely and productively within agreed guidelines.

References

Attai, L. (2018) *Student data privacy*. 1st edn. London: Rowman and Littlefield.

Department for Education (2016) *Keeping children safe in education*, *Assets.publishing.service.gov.uk*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf (Accessed: 6 June 2018).

Department for Education (2018) *Keeping children safe in education*, *Assets.publishing.service.gov.uk*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707761/Keeping_Children_Safe_in_Education_-_September_2018.pdf (Accessed: 6 June 2018).

HM Government (2015) *Counter-Terrorism and Security Act 2015, GOV.UK*. Available at: https://www.gov.uk/government/collections/counter-terrorism-and-security-bill (Accessed: 6 June 2018).

HM Government (2016) *Revised Prevent Duty Guidance: for England and Wales*, *Assets.publishing.service.gov.uk*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf (Accessed: 6 June 2018).

Hunter, N. (2012) *Internet safety*. 1st edn. London: Raintree Press.

Information Commissioner's Office (2018) *Education and families*, *Ico.org.uk*. Available at: https://ico.org.uk/for-organisations/education/ (Accessed: 6 June 2018).

Jenkins, H. (2008) *Convergence culture*. 1st edn. New York (NY): New York University Press.

Lau, W. (2017) *Teaching computing in secondary schools*. 1st edn. Abingdon: Routledge.

Lock, J. (2018) *GDPR for schools: how will the new data regulations affect my school?*, *Tes.com*. Available at: https://www.tes.com/news/gdpr-schools-how-will-new-data-regulations-affect-my-school (Accessed: 6 June 2018).

NSPCC (2017) *E-safety for schools*, *NSPCC*. Available at: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/ (Accessed: 6 June 2018).

Ribble, M. (2015) *Digital citizenship in schools*. 3rd edn. New York, NY: ISTE Books.

Rooney, A. (2014) *Internet safety*. 1st edn. London: Franklin Watts.

Stowell, L. (2016) *Staying safe online*. 1st edn. London: Usbourne.

UK Council on Child Internet Safety (2016) *Education for a connected world*, *Assets.publishing.service.gov.uk*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF (Accessed: 6 June 2018).

UK Safer Internet Centre (2018) *Appropriate Filtering*, *Saferinternet.org.uk*. Available at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering (Accessed: 6 June 2018).