Keeping children safe in education—schools and colleges proposed revisions 2022—defend digital me (DDM)

About defend digital me
defenddigitalme is a not-for-profit organisation. We advocate to protect children's rights to privacy and safe, fair and transparent data processing in education, in England, and beyond.

We respond to address only the final question: Filtering and monitoring systems
Question 29: Do you feel able to make informed decisions on which filtering and monitoring systems your school or college should use?

1. Summary

We wish to secure a commitment by the DfE to reconsider the current guidance on this issue following a dedicated engagement with stakeholders.

DDM is concerned by the current legal framework governing the widespread monitoring of children's digital activities by schools and other education providers.

DDM considers that the current legal framework for the monitoring of digital activities by schools is resulting in ongoing interferences with rights under Article 8 of the European Convention on Human Rights (**"ECHR"**) that are not "in accordance with the law".

DDM's concerns arise in the context of a noticeable scope creep in this space since the DfE published its KCSIE Guidance in 2016 following a consultation. In recent years, proactive monitoring of all digital activities has become the rule rather than the exception. And new practices – such as automated profiling or monitoring personal devices – are becoming more and more widespread.

2. Stakeholder support

Stakeholders have requested greater clarity on the lawful boundaries of digital monitoring. The May 2016 Full Government Response to the KCSIE consultation recorded the breakdown of 288 responses on the question of *"Would it help schools and colleges if online guidance/ an online portal was created that set out what "appropriate" filters and monitoring systems look like and advice on how to satisfy themselves that they have them?"*. 250 stakeholders (87%) answered that question with a "yes". However, very little assistance was provided in the updated KCSIE guidance that followed (and which forms the basis of the current iteration).

Stakeholder concerns with the legal framework continue to the present day and are shared by companies that provide the monitoring technologies used by schools. For example,

Registered company number 11831192 | For more information please see https://defenddigitalme.org/

Opendium, a leading provider of internet filtering and monitoring solutions, has blogged about views expressed at a 2019 conference held by the Police Service's Counter Terrorism Internet Referral Unit:[1]

> *A big concern that repeatedly came up in the breakout discussions was the rather woolly guidance from the Department for Education when it comes to online safety. Indeed, Keeping Children Safe in Education distils the huge subject of online safety down to just 3 pages: the infamous "Annex C".*
>
> *The UK Safer Internet Centre has added some additional guidance, but fundamentally, phrases such as "to what extent does the filter system block inappropriate content via mobile and app technologies" and "the school should carefully consider how [3G and 4G internet access] is managed on their premises" are not terribly helpful. We pushed the point that schools really do need better advice.*

3. Legal framework

Statutory duties

Digital monitoring is conducted pursuant to various statutory duties. These duties are:

3.1 For all education providers, Section 26 of the Counter Terrorism and Security Act 2015 (the so-called **"Prevent Duty"**): which requires *"specified authorit[ies]"* to *"in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism".*

3.2 For maintained schools and relevant further education providers, Section 175 of the Education Act 2002: which requires local authorities to *"make arrangements for ensuring that their education functions are exercised with a view to safeguarding and promoting the welfare of children"*, for governing bodies to *"make arrangements for ensuring that their functions relating to the conduct of the school are exercised with a view to safeguarding and promoting the welfare of children who are pupils at the school"*, and for governing bodies of relevant further education institutions to *"make arrangements for ensuring that their functions relating to the conduct of the institution are exercised with a view to safeguarding and promoting the welfare of children receiving education or training at the institution"*. Pursuant to Section 175(4), *"in considering what arrangements are required to be made"*, education providers shall "*have regard to any guidance given from time to time (in relation to England) by the Secretary of State"*.

---

[1] Opendium blog, "Safeguarding and Counter Terrorism Conference Report"; available at https://www.opendium.com/blogs/safeguarding-and-counter-terrorism-conference-report; emphasis added.

3.3 For independent schools and academies, §§6-8 of Part 3 of Schedule 1 to the Education (Independent School Standards) Regulations 2014: which require proprietors to ensure *"arrangements are made to safeguard and promote the welfare of pupils at the school"*, and that *"such arrangements have regard to any guidance issued by the Secretary of State".*

3.4 For non-maintained special schools, §3 of Part 1 of Schedule 1 to the Non-Maintained Special Schools (England) Regulations 2015, proprietors *"must make arrangements for safeguarding and promoting the health, safety and welfare of registered pupils at the school which— (a) have regard to any guidance… about safeguarding and promoting the health, safety and welfare of pupils …"*.

3.5 Prevent Duty Guidance

In relation to the Prevent Duty, the Home Office has promulgated "Revised Prevent duty guidance: for England and Wales" (**"the Prevent Guidance"**) (updated April 1, 2021). Whilst the Prevent Guidance contains a single paragraph (§45) directed to "filtering solutions", it does not at all address the related issue of monitoring.

3.6 KCSIE Guidance

As per the various provisions above, arrangements made pursuant to these statutory duties must be exercised subject to relevant statutory guidance issued by the Secretary of State. The guidance in the monitoring context is the KCSIE Guidance**.** The KCSIE Guidance has recently been updated (from 1 September 2021).

Monitoring is predominantly dealt with in the KCSIE Guidance at §§122-130. In particular, §§129-130 provide:

> *128. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.*
>
> *129. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.*

4. UK Safer Internet Centre Guidance

As indicated in the KCSIE Guidance, education providers may benefit from considering UK Safer Internet Centre (UKSIC) guidance on "Appropriate Filtering and Monitoring" (**"UKSIC Guidance"**). UKSIC is a partnership of three organisations: Childnet International, Internet Watch Foundation and South West Grid for Learning (SWGfL).

The UKSIC Guidance on monitoring states at a high level that *"[t]here are a range of monitoring strategies and systems however the appropriate monitoring strategy selected should be informed by your risk assessment and circumstances. It is also vitally important to also review and refine the relevant policies as part of assessing (or implementing) a monitoring strategy or system."* The Guidance then goes on to consider types of monitoring activities, content that should be subject to monitoring, and principles that should be considered when designing monitoring strategies.

5. Article 8 interferences

Requirement that Article 8 ECHR interferences are 'in accordance with the law'

There is no doubt that monitoring by schools will constitute an interference with children's rights under Article 8 ECHR. DDM's concerns are that those interferences are often not "in accordance with the law". The relevant principles for this requirement under the Convention have been summarised by the Divisional Court in *R (Bridges) v South Wales Police* [2019] EWHC 2341 (Admin), at §80 in an Article 8 ECHR context in relation to the use by police of automated facial recognition technology by the police:

> *The general principles applicable to the 'in accordance with the law' standard are well-established: see generally per Lord Sumption in Catt, above, [11]-[14]; and in Re Gallagher [2019] 2 WLR 509 at [16] – [31]. In summary, the following points apply.*
>
> *(1) The measure in question (a) must have 'some basis in domestic law' and (b) must be 'compatible with the rule of law', which means that it should comply with the twin requirements of 'accessibility' and 'foreseeability' (Sunday Times v United Kingdom (1979) 2 EHRR 245; Sliver v United Kingdom (1983) 5 EHRR 347; and Malone v United Kingdom (1984) 7 EHRR 14).*
>
> *(2) The legal basis must be 'accessible' to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must also be 'foreseeable' meaning that it must be possible for a person to foresee its consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself' (Lord Sumption in Re Gallagher, ibid, at [17]).*

(3) Related to (2), the law must 'afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise' (S v United Kingdom, above, at [95] and [99]).

(4) Where the impugned measure is a discretionary power, (a) what is not required is 'an over-rigid regime which does not contain the flexibility which is needed to avoid an unjustified interference with a fundamental right' and (b) what is required is that 'safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights' (per Lord Hughes in Beghal v Director of Public Prosecutions [2016] AC 88 at [31] and [32]). Any exercise of power that is unrestrained by law is not 'in accordance with the law'. Judgment Approved by the court for handing down. R (Bridges) -v- CC South Wales & ors

(5) The rules governing the scope and application of measures need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them (per Lord Sumption in Catt at [11]).

(6) The requirement for reasonable predictability does not mean that the law has to codify answers to every possible issue (per Lord Sumption in Catt at [11]).

Although the Divisional Court's conclusions on whether the interference in that case was in accordance with the law were not shared by the Court of Appeal, it did not however did not dispute this summary of the relevant principles (2020] EWCA Civ 1058, at §55).

There are two important points from the Court of Appeal's *Bridges* judgment of particular importance in these circumstances. First, the Court accepted at §§82-83 that, when considering the "in accordance with the law" test, a "relativist" approach applies – i.e. that *"the more intrusive the act complained of, the more precise and specific must be the law said to justify it"*. Second, it is clear from the Court's judgment (see §104) that, in scenarios that involve monitoring/surveillance, the operation of data protection legislation will not by itself satisfy the "in accordance with law" requirement.

More recently, in *R (A) v Secretary of State for the Home Department* [2021] UKSC 37, at §52, the Supreme Court has commented that the "in accordance with the law" requirement does not (emphasis added): *"require the elimination of uncertainty, but is concerned with ensuring that law attains a reasonable degree of predictability and <u>provides safeguards</u> against arbitrary or capricious decision-making by public officials".* To the same effect, see *Bărbulescu v Romania* [2017] ECHR 742, at §120, where the Grand Chamber made clear that, where Article 8 interferences occur at a horizontal level, *"adequate and sufficient*

safeguards against abuse" are required, particularly where monitoring is intrusive (as is the case here).

6. defenddigitalme concerns

DDM considers that the current legal framework for monitoring is not in accordance with the law and that the KCSIE Guidance is irrational.

6.1 The legal framework is not in accordance with the law

In reaching this conclusion, DDM considers that the "relativist" approach endorsed by the Court of Appeal in Bridges weighs in favour of a more rigorous standard in these circumstances. In particular because:
(a) children are the subject of monitoring and merit greater protection in a privacy context;
(b) given the power imbalance between pupils/parents and schools, consent to monitoring is incredibly difficult to withhold;
(c) content that is monitored is often highly sensitive (e.g. see the "monitoring content" table in the UKSIC Guidance; or a recent DCMS report recording that *"Safety tech companies handle highly sensitive, personal and often harmful data*");[2]
(d) monitoring is often incredibly intrusive, both in term of intensity (i.e. significant amount of personal information is processed)[3] and duration (e.g. beyond school hours);
(e) school staff are (understandably) not experts in the field of digital monitoring: they are therefore not equipped to deal with relevant technologies or the outcomes from those technologies;[4]
(f) monitoring is often outsourced to third parties, notwithstanding the lack of any obvious statutory duty of care on the part of such third parties;
(g) monitoring is often undertaken by novel technologies including 'artificial intelligence' and algorithmic decision making; and (e) monitoring may result in significant interferences with *other* fundamental rights, in particular rights to freedom of expression (via a chilling effect),[5] and the prohibition on discrimination (e.g. through children's changing use of slang and

---

[2] DCMS, "Safety Tech in the UK: Skills and Capabilities"; available at https://www.gov.uk/government/publications/safety-tech-in-the-uk-skills-and-capabilities/safety-tech-in-the-uk-skills-and-capabilities.

[3] Smoothwall FAQs (accessed November 30, 2021) Does Monitor Managed Service capture bank details and passwords? https://kb.smoothwall.com/hc/en-us/articles/360002135724-Frequently-Asked-Questions-FAQs-

[4] UKSIC itself notes, "logfile information … can often be difficult to understand and may require specialism to analyse"; see https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring.

[5] The 2016 UN joint declaration on Countering Violent Extremism and Freedom of Expression, concluded that "Countering Violent Extremism" programmes and initiatives "have in some cases impacted negatively on academic freedom and open debate in schools and universities, undermining the freedom of expression rights of children and young people" and that programmes "generally offer insufficiently clear definitions of "extremism" or "radicalisation". See https://www.osce.org/files/f/documents/e/9/237966.pdf.

foreign languages (e.g. discrimination against Muslim pupils in the context of the Prevent Duty or the Equality Act 2010).

In terms of the legal framework described above: (a) the statutory duties themselves do not contain any safeguards; (b) the Prevent Guidance is silent on monitoring; and (c) the handful of paragraphs in the KCSIE Guidance (§122-130) is incredibly vague.

The UKSIC Guidance provides slightly more detail. However, unlike the Prevent and KCSIE Guidance, the UKSIC Guidance is not statutory guidance, which education providers are required by law to have regard to. In any event, the UKSIC Guidance is still itself overly generic. It fails to consider key areas where disproportionate interferences with Article 8 ECHR and other Convention rights are likely to be most common and/or serious.

6.2 DDM has identified eight areas with the legal framework where necessary safeguards in statute or guidance are worryingly absent

6.2.1 24/7 monitoring

DDM's investigations into monitoring by schools indicate that systematic, uninterrupted monitoring is widespread.

For example, eSafe, a major provider of monitoring software (purchased in June 2021 by Smoothwall) promoted its ability to "monitor users inside and outside of education hours, in term time and holidays too".

The same appears true of another major provider, Netsweeper, which permits offline monitoring.[6]

It is unclear whether pupils and parents will have a reasonable expectation that monitoring pursuant to education providers' statutory duties will take place before or after the school day, at weekends or during the holidays; all times at which education providers statutory duties do not obviously apply.

A poll of 1,004 parents commissioned by DDM in 2018 recorded how the majority of respondents agreed parental consent should be obtained for "[i]nternet Monitoring software that can be run remotely at home in the evenings or during school holidays".[7]

---

[6] Netsweeper website available at https://www.netsweeper.co.uk/student-device-filtering/

[7] DDM commissioned Survation to conduct an online poll of 1,004 parents of children aged 5-18 in state school in England, 17th-20th February 2018. See https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf for the results.

The legal framework fails to address whether out-of-school monitoring: (a) is ever lawful (noting here the ECtHR has held that automatic, unconditional monitoring of prisoners' communications, without any judicial oversight, is not itself "in accordance with the law": Petra v Romania [1998] ECHR 93); and (b) if sometimes lawful, an indication of where it will be proportionate/disproportionate. The importance of this issue was recognised by the previous (2020) iteration of the KCSIE guidance (at §92; emphasis added), which stated "Additional information to support governing bodies and proprietors keep their children safe online (including when they are online at home) is provided in Annex C." However, no such guidance was contained in that Annex. Furthermore, this reference to monitoring when pupils are at home has now been cut from the updated KCSIE guidance.

6.2.2 Personal Devices

DDM's investigations have revealed that many education providers employ what is known as a "BYOD" (Bring Your Own Device) policy, meaning that private phones, tablets and laptops can be used by pupils at school.[8] These policies are usually subject to a requirement that monitoring software is installed on private devices. For example, Impero, one of the largest monitoring solutions providers, says that it *"supports non-school-owned devices or home devices"*.[9] The UKSIC Guidance on BYOD monitoring is incredibly vague. It does not at all address the circumstances in which BYOD monitoring may exceed individuals' reasonable expectations of privacy and may therefore be unlawful (something which overlaps substantially with questions of 24/7 monitoring). For example, one question to address is the way in which BYOD monitoring might interfere with the privacy rights of other individuals who share personal devices (e.g. where a family only has one iPad), and whom are not the subject of safeguarding duties. In this regard, the ECtHR has made clear in *Amann v Switzerland* [2000] ECHR 88 that legal provisions giving rise to monitoring may not be "in accordance with the law" if they do not contain safeguards for those who are monitored *"fortuitously"*. The UKSIC Guidance raises BYOD as am issue, but offers no meaningful advice: "*if the system includes the capability to monitor personal mobile and app technologies (ie not owned by the school), ensure it is deployed in accordance with policy and how data is managed. Does it monitor beyond the school hours and location*".

6.2.3 Monitoring of third-party communications

Schools and education providers will also conduct monitoring of 3rd party communications sent to monitored devices – e.g. a parent contacting their child. These are individuals who, as per *Amann*, are monitored *"fortuitously"*. However, there is nothing in the guidance

---

[8] From responses given to freedom of information requests in 2017, of the 400 sample schools chosen at random geographical spread across England using monitoring software, defenddigitalme estimates that at least 50% of schools in England may apply Bring Your Own Device (BYOD) policies

[9] Impero website available at https://support.imperosoftware.com/support/solutions/articles/44002201187-impero-classroom-best-practices-for-non-school-owned-devices

which addresses this privacy risk of tools designed to actively work around encrypted content.

6.2.4 Webcam monitoring: live and capturing still images from it

Live monitoring of children's activities via webcams is widespread. For example, NetSupport DNA's website explains how "[w]hen a critical safeguarding keyword is copied, typed or searched for across the school network, schools can turn on NetSupport DNA's webcam capture feature…to capture an image of the user (not a recording/video) who has triggered the keyword. …*This feature is common across most solutions in the sector*…"[10] This form of monitoring likely goes beyond pupils' and parents' reasonable expectations of privacy, particularly where that monitoring is covert. It will therefore often result in invasive interferences with ECHR Article 8 rights. Yet this issue is not addressed at all by the legal framework.

6.2.5 Reviewing images in particular by commercial third parties

Over 300 school policies reviewed by defenddigitalme are not specific as to *who* may view images which have been captured by monitoring solutions. The images may be viewed by an undetermined and potentially unlimited number of persons within a school, its support services, or at the company contracted to carry out the service (including employees based outside the UK). The potential sensitivity of images should not be underestimated given the questions of the nature of monitoring on BYOD, and out of hours monitoring, which could feasibly include consensual conversations between older teens in sexual relationships. The legal framework is silent on this issue.

6.2.6 Consent and lack of transparency

DDM understands that consent is the predominant "lawful basis" on which personal data is processed as part of digital monitoring. It is concerned by three recurring issues that arise in relation to consent and the lack of transparency when consent is purportedly provided. None of these issues are addressed by the relevant guidance.

As recognised in the data protection context (GDPR Recital 43), consent may not be valid where there is a clear power imbalance between a data controller and data subject. That point has been recognised in an education setting by the Swedish Data Protection Authority, where it fined a secondary school for conducting a facial recognition class registration pilot

[10] Emphasis added; available at https://web.archive.org/web/20210416105746/http://www.netsupportdna.com/education/safeguarding.asp

on the basis of consent because *"students are in a position of dependence which results in a substantial imbalance"*.[11]

The most common issue revealed by DDM research is that education providers regularly make access to the Internet contingent upon acceptance of the school policy in a pupil agreement; rendering any consent invalid, both in respect of the GDPR and ECHR. For example, the consent statement for one school reads: "*If you wish your child to gain access to the Internet, please carefully read, sign and return the following agreement to your form tutor at school.*"[12]

Consent is often lacking in transparency (something the ECtHR has recognised as particularly important in a surveillance context: see *Bărbulescu v. Romania* [2017] ECHR 754). For example, the SWGFL "Acceptable Use Policy" template, which the UKSIC Guidance refers to at fn.8, suggests the following consent wording: *"I understand that the school / academy will monitor my use of the systems, devices and digital communications."* This wording does not address how monitoring will take place, by whom, when, and what the consequences may be. For example, the consent statement for any given pupil reads: "*for my own personal safety: I understand that the school will monitor my use of the systems, devices and digital communications*". Whilst another statement from the Chesterfield College Group reads: *"[i]nternet usage is appropriately monitored on all College Group provided internet enabled devices, in line with data protection, human rights and privacy legislation."*[13]

DDM's investigations indicate that parents are often uniformed of monitoring that goes on; something that is particularly important where young children are the subject of monitoring. DDM's 2018 survey (via Survation) recorded that 46% of parents were not offered any choice to have monitoring solutions imposed on their children. In the same poll, 37% of parents did not know whether their child's school used monitoring and keylogging software (i.e. software that captures children's search terms). Whilst over 80% of parents agreed in relation to keylogging systems that parents should be informed of which words are flagged and what the consequences might be for their child if their searches are flagged.

---

[11] See "Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students", p.4; available at https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf.

[12] See https://www.whatdotheyknow.com/request/730260/response/1784311/attach/html/3/Acceptable%20use%20of%20IT%20Policy%20for%20Pupils%20May2018%201.docx.html

[13] See https://www.whatdotheyknow.com/request/730258/response/1825282/attach/2/GOV12 Online Safety Policy draft.pdf

6.2.7 Data sharing (e.g. with police or the Prevent programme)

DDM is aware of at least one data sharing agreement between monitoring service providers and the police: between the Metropolitan Police, CTIRU and SWGfL.[14] The legal framework does not at all address these types of agreements, even though they may have serious impacts on pupils whose data is shared and will often go beyond their reasonable expectations of how information obtained from monitoring will be used. Nor are there any safeguards in the legal framework to ensure specified authorities know when data sharing in pursuit of the Prevent duty are permissible.

6.2.8 Use of AI, machine learning and other algorithm-based monitoring services

A recent DCMS report states that *"[m]uch of safety tech is driven by machine learning"*. For example, the major provider Smoothwall offers "Signal", a product which *makes use of "advanced AI capabilities."*[15]

The use of novel technologies of this sort comes with a range of risks. In particular: (i) the risk of discrimination (it is widely recognised that machine learning has the potential to amplify existing biases[16]); and (ii) a lack of transparency – both in terms of students' failure to understand what type of monitoring is taking place, as well as teachers' ability to understand how new technologies operate. The legal framework does not address circumstances in which such technologies should be used and the safeguards that should be employed where they are (e.g. mechanisms for addressing algorithmic errors or the need for human input when such technologies are used).

5. Conclusion and next steps

In light of serious shortcomings with the legal framework, DDM suggests the viable way forward is for the Department for Education to commit to amending and/or providing further, new guidance following a process of thorough dedicated engagement with stakeholders. These updates should provide necessary clarity to schools, technology providers, and—most importantly— respect the rights of children and families.

March 10, 2022

---

[14] Information sharing agreement between the Metropolitan Police, UKSIC, SWGfL and Plymouth University, http://whatdotheyknow.com/cy/request/401426/response/1011703/attach/3/ISA MPS CTIRU List signed redacted version 25 07 17.pdf

[15] See https://us.smoothwall.com/tech-resource-hub/articles/smoothwall-acquires-future-digital-2/

[16] CDEI (2020) Review into bias in algorithmic decision-making https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making/main-report-cdei-review-into-bias-in-algorithmic-decision-making