
Has your child been signed up by their school to any app, technology, or online system that uses personal data?
- YES: 53%
- 24% don't know

Which of the following does the school use your child’s personal data for?
- School admin systems (absence, sickess reporting, census reporting, classroom seating, cashless systems): 82%
- Online teaching and learning systems (homework apps, sharing files via Google and Microsoft type platforms): 72%
- Behavioural monitoring, profiling or safeguarding (CCTV, Internet search monitoring and keylogging, cashless catering, profiling library books read and behaviour points): 47%

Does your school use any of the following systems?
- CCTV / IPTV closed circuit or surveillance cameras: 53%
- Internet monitoring and keyword recording software (records children's online Internet use): 46%
- Any other biometric technology (fingerprints, retinal and palm scans, facial image recognition): 25%
- 25% don't know

Survation asked 1,004 respondents in total online, between 17th and 20th February 2018. All respondents were parents of state-educated children age 5-18. These respondents were asked detailed questions about their child's personal data in school, their understanding of which technologies were used, as well as overarching questions about their attitudes towards the use of children's personal confidential data at national level by third parties. Personal data was defined as any information that can be used to identify a child.
The Department for Education has a database of over 20 million children’s named personal records called the National Pupil Database, collected since 2002. From there the Department for Education can give children’s data collected to third-parties. Have you been informed that the Department for Education may give your child’s data to third-parties?

If you had the opportunity to see your child’s named record from the National Pupil Database, would you choose to see it?

Today the Department for Education refuses children and parents the right to see their own record, check it is accurate or have data corrected. defenddigitalme is campaigning to have that changed, and wants the government to respect children’s Subject Access Rights and Recital 63 in the General Data Protection Regulation.
Do you believe children should be able to consent on their own in school to the use of their personal data by third parties (e.g. companies and researchers)?

Is the current amount of control you have over your child's digital footprint sufficient?

You said that your school uses Internet Monitoring and keylogging software. Were you offered a choice to use this or not?

Does the Internet Monitoring software used by the school....

Log children's Internet search terms and create flags based on keywords?

Record screen content as created / seen by the child?

Record children's image through the webcam?

''defenddigitalme believes that parents and children have lost control and oversight of their child's digital footprint in education, even by their fifth birthday.''

defenddigitalme.com
You said your school uses biometric technology. Were you offered a choice whether to use this system or not?

**NO 38%**
defenddigitalme believes a Code of Practice is needed that covers use of children's biometrics and better data protection practice. The 2012 Protection of Freedoms Act requires both parents and the child to be asked for consent to use a child's biometrics, and an alternative method to be on offer.

Were you informed of how long the fingerprint, retinal scan, palm scan or facial image recognition data are kept by either the school or the company that provides the service?

**NO 50%**

It is a basic Principle of data protection law today, to communicate well with the people whose personal data that are being processed, for processing to be fair and lawful. That includes how long you plan to hold data for and to ensure that retention periods are respected. This is a key issue for maturing school systems and the rights and responsibilities of parents and schools today.