Who needs to be told what? What schools must do to meet their duties on data protection and privacy.

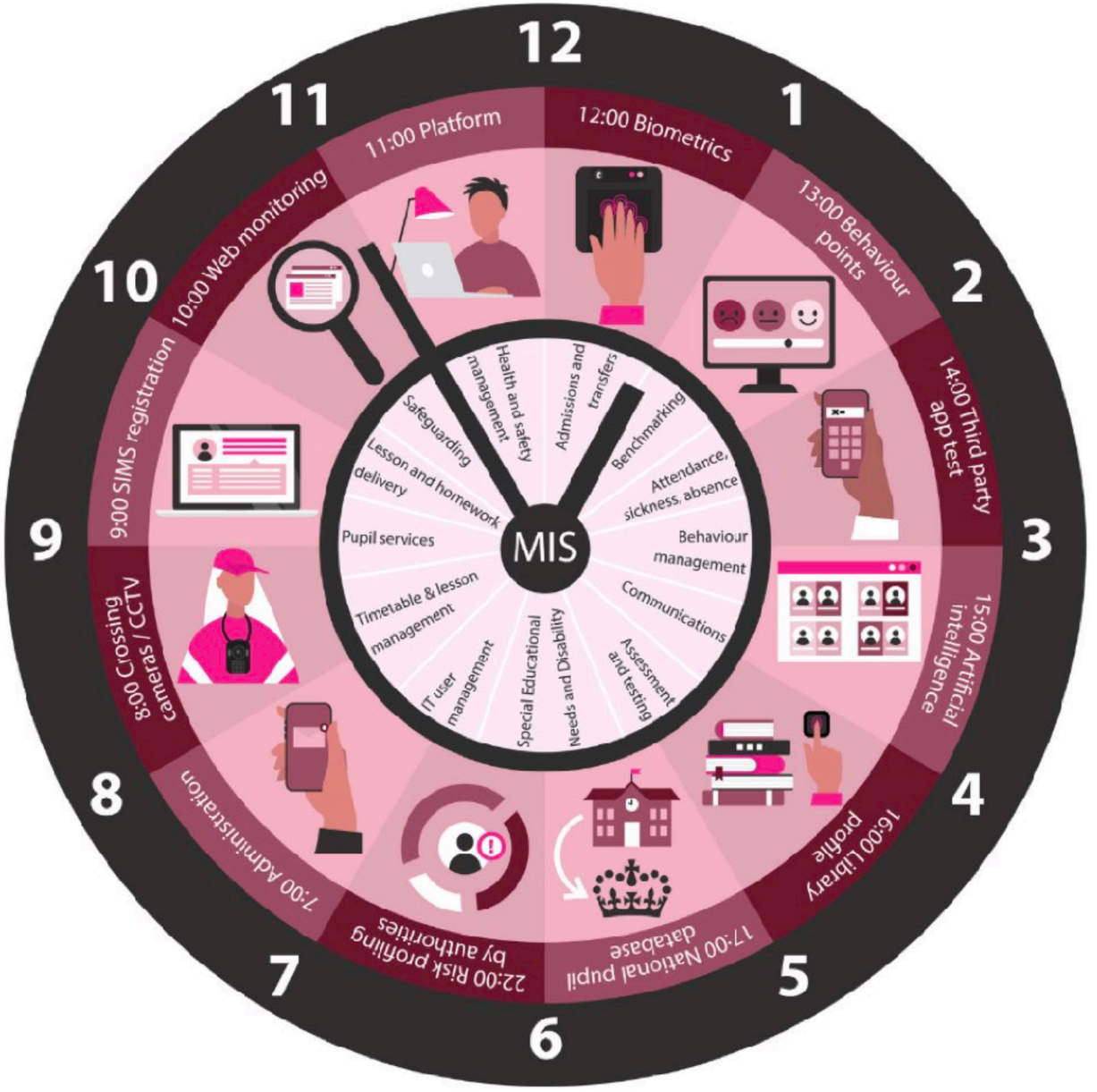
The Schools & Academies Show, Birmingham
November 2019
defenddigitalme.com

“The sensitivity of digitized pupil and student data should not be underestimated”

International Working Group on Data Protection in TelecommunicationsWorking Paper on e-Learning Platforms
(April 2017)

Who Needs to be Told What? What Schools Need to Do to Meet their Duties on Data Protection and Privacy

- What does a day-in-the-life of a datafied child look like at your school, and can you explain it?
- Do you understand how the National Pupil Database works and what you need to tell families?
- What impact do emerging technologies have on your data processing duties?
- Case studies from legal challenges and regulatory enforcement
- Security and privacy: How not to be the next news story



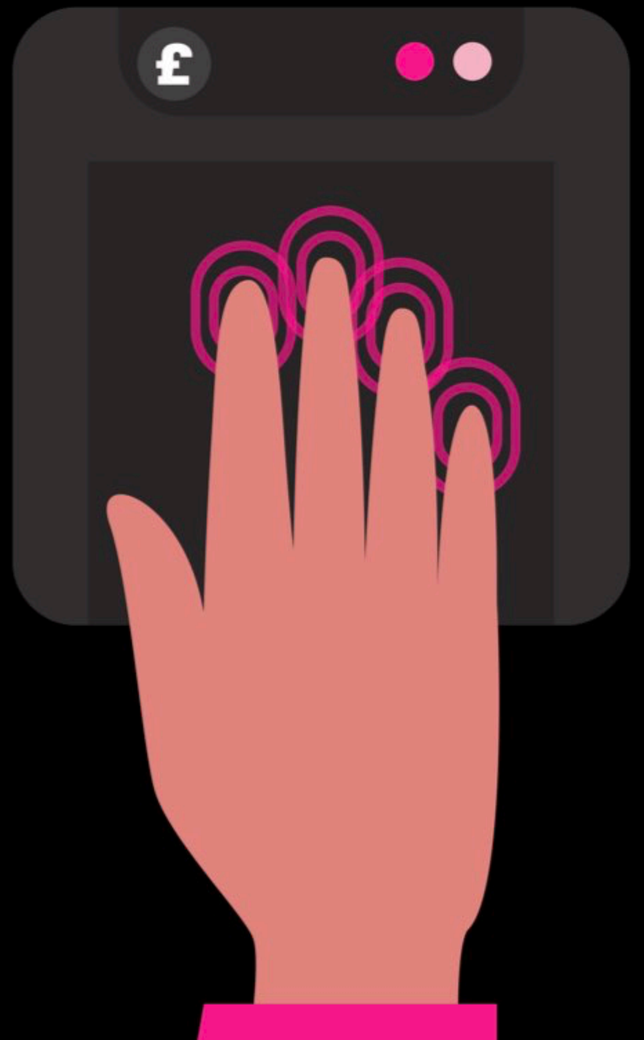
defenddigitalme.com
#MyRecordsMyRights

What does a day-in-the-life of a datafied child look like at your school, and can you explain it?

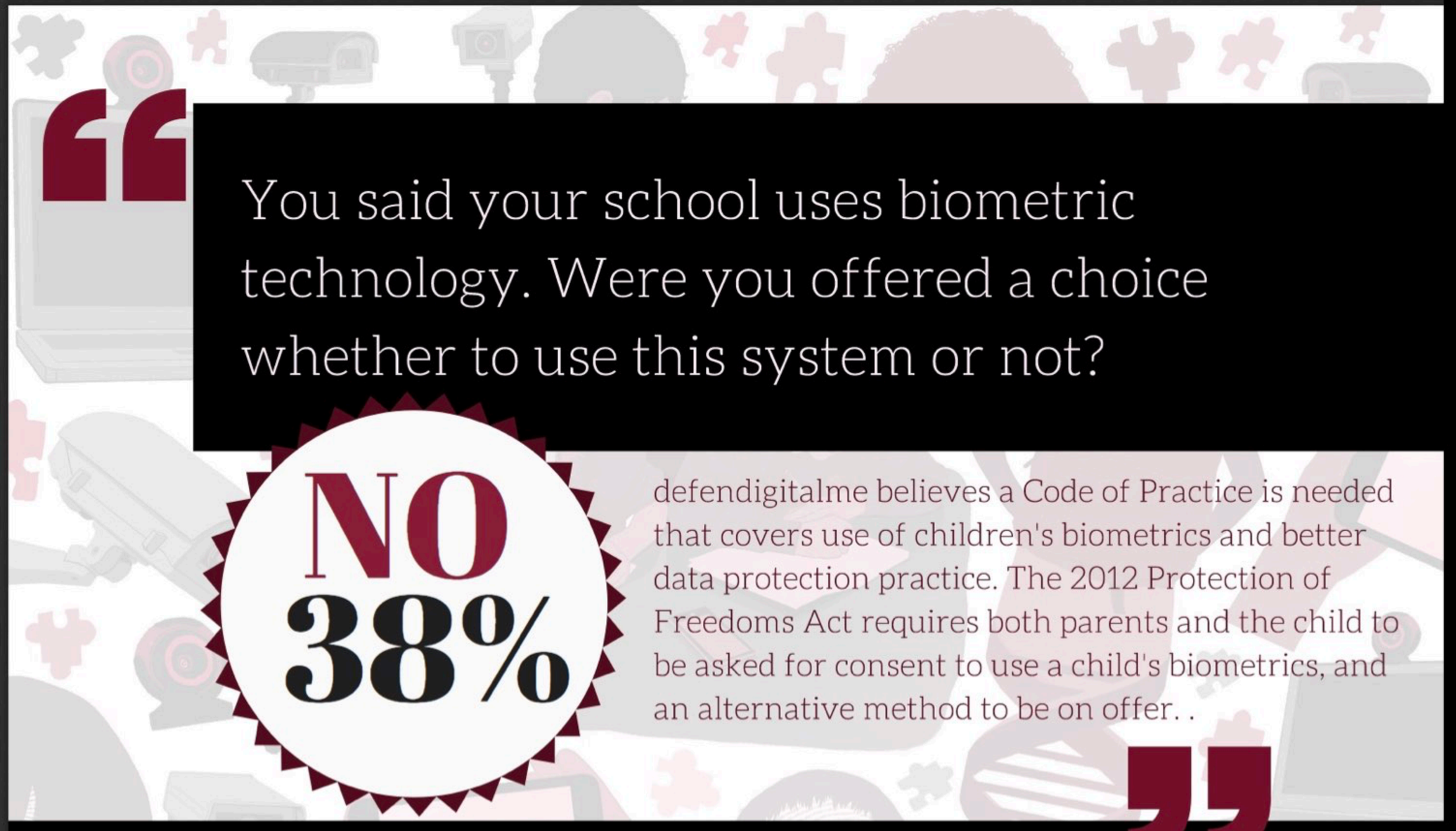
Cashless catering systems connected to biometric identity systems

There is no requirement to ask for consent to capture a child's biometrics in school in England / Wales / Scotland / Northern Ireland?

True or false?



State of Data survey of 1,004 parents (February 2018)



“Children do not lose their human rights by virtue of passing through the school gates”

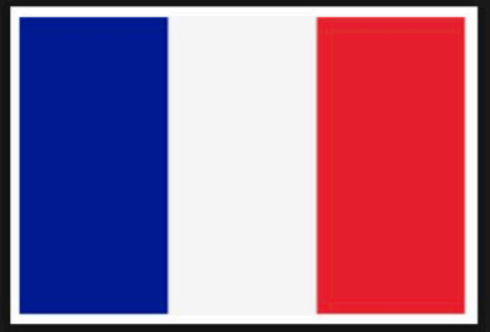
UN Committee on the Rights of the Child, on ‘The aims of education’, 2001

Insufficient legal basis for data processing (Art. 5 (1) c) GDPR, Art. 9 GDPR, Art. 35 GDPR, Art. 36 GDPR)

A school in Skellefteå, Sweden, made a trial to use facial recognition technology. The fine was imposed against the school which had used facial recognition technology to monitor the attendance of students. Even though, in general, data processing for the purpose of monitoring attendance is possible doing so with facial recognition is disproportioned to the goal to monitor attendance. The supervisory authority is of the opinion that biometric data of students was processed which is why Art. 9 GDPR is applicable. Additionally, the authority argued that consent can not be applied since students and their guardians cannot freely decide if they/their children want to be monitored for attendance purposes. When examining if the school board can rely on any of the exemptions listed in Art. 9 (2), the supervisory authority found that this was not the case. The supervisory authority also found that there was a case of a processing activity with high risks since new technology was used to process sensitive personal data concerning children who are in a dependency position to the high school board and due to camera surveillance being used in the students everyday environment. In the view of the authority, the school board was not able to demonstrate compliance with Art. 35 GDPR and that the school board was required to consult the authority in accordance with Art. 36 (1) GDPR.

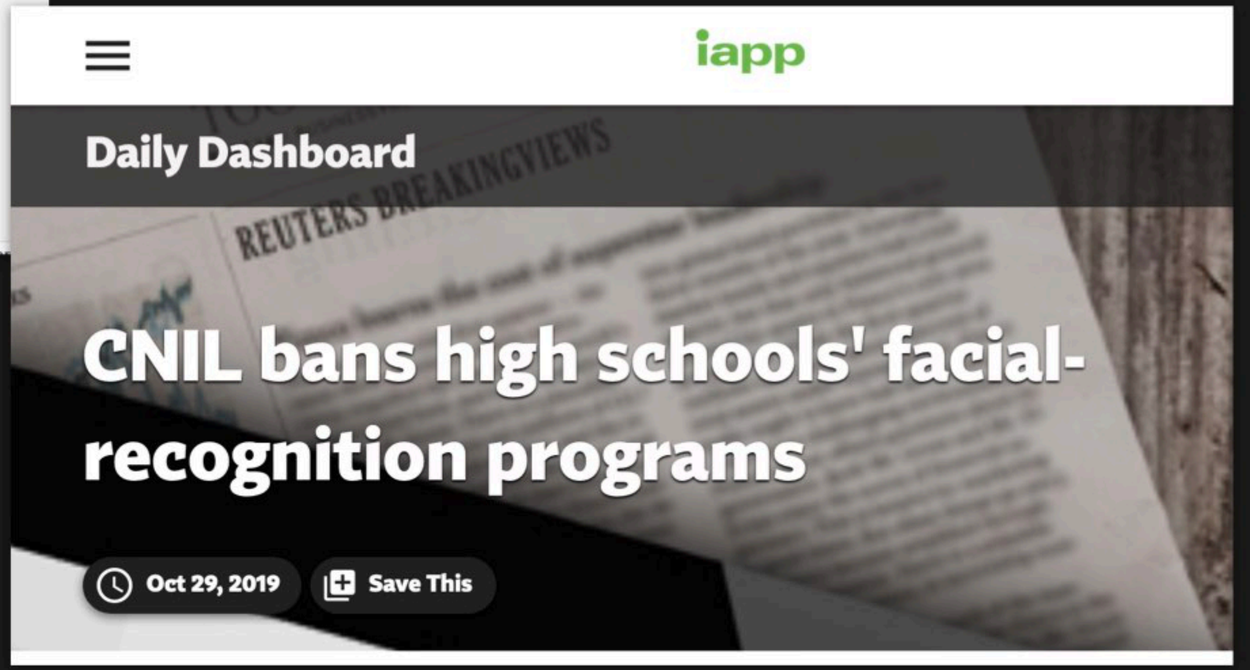
School in Skellefteå
Data Protection Authority of Sweden
August 2019
Fine: 18,630 Euros

Failure of Fundamental Principles: proportionality and necessity



Facial recognition is too invasive.

'the goals the facial-recognition program would help reach, could "be achieved by much less intrusive means in terms of privacy and individual freedoms.'"



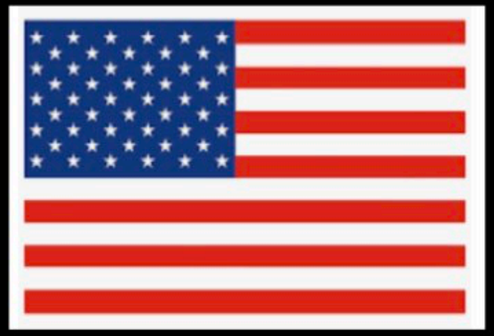
Insufficient technical and organisational measures to ensure information security (Art. 32 GDPR)

Fine for security vulnerabilities in a mobile messaging app developed for use in an Oslo school. The app allows parents and students to send messages to school staff. Due to insufficient technical and organisational measures to protect information security, unauthorised persons were able to log in as authorised users and gain access to personal data about students, legal representatives and employees.

Oslo Municipal Education Department
Norwegian Supervisory Authority (Datatilsynet)
April 2019
Fine: 203,000 Euros

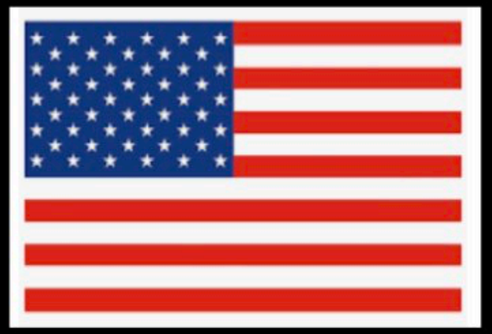
New York’s student data laws on security

New York’s Student Data law includes a specific requirement to encrypt student data in line with the encryption requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) (N.Y. Educ. Law § 2-D(5)(f)(5)).



What about legal basis and consent (Art. 6 GDPR)

Montgomery County Public Schools,
Maryland U.S.
October 2019
162,680 pupils (2018–2019)



MONTGOMERY COUNTY PUBLIC SCHOOLS
Online Digital Tools Consent Form

Dear Parents and Guardians,

MCPS teachers may utilize a variety of supplemental online digital tools to reinforce the district's instructional program. In the list below, you will find supplemental tools that may be used by teachers. These tools have been evaluated to be safe for student use and are consistent with federal laws on student data privacy.

ABC Mouse	Educreations	IXL	Quizalize	Storyboard That
ABCya	Epic!	Kahoot	Quizizz	Thinglink
Animoto	Everfi	Khan Academy	Quizlet	Toontastic
BookCreator	Figure	Menti/Mentimeter	Reason Compact	Typing Club
Canva	Flipgrid	Opinion	Remind	Unity
ClassDojo	Freckle Math	Padlet	Scratch	UnStuck
Code.org	Glogster.edu	Pear Deck	Scratch Jr.	Vocaroo
Conjuguemos	Goosechase	Playground Physics	Screencastify	Weebly
CoSpaces EDU	HP Reveal	Playposit	Seesaw	Wixie
Desmos	iCivics	Poll Everywhere	Socrative	XtraMath
Doodle Buddy	Incredibox	Powtoon	Splash Math	
Edpuzzle	Insta360 ONE X	Prodigy	Splice	

MCPS requests your consent to allow your student to use the supplemental tools listed above, as these tools may collect personally identifiable student information, such as first and last name, classroom teacher, or grade level. This information is typically collected by online digital tools to enable use of the tool and to track student progress.

Descriptions of the above supplemental tools are provided on the following pages. Links to each supplemental tool's terms of service and privacy policy, as well as additional information on MCPS' data privacy practices, are available on the MCPS Data Privacy and Security website[1].

If you choose not to provide consent for your student to use the above tools, alternative instructional activities will be provided.

Yes, I consent to my student's use of the supplemental online digital tools listed above	☐
No, I do not consent to my student's use of the supplemental online digital tools listed above	☐

Student Name: _____

Student ID Number: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

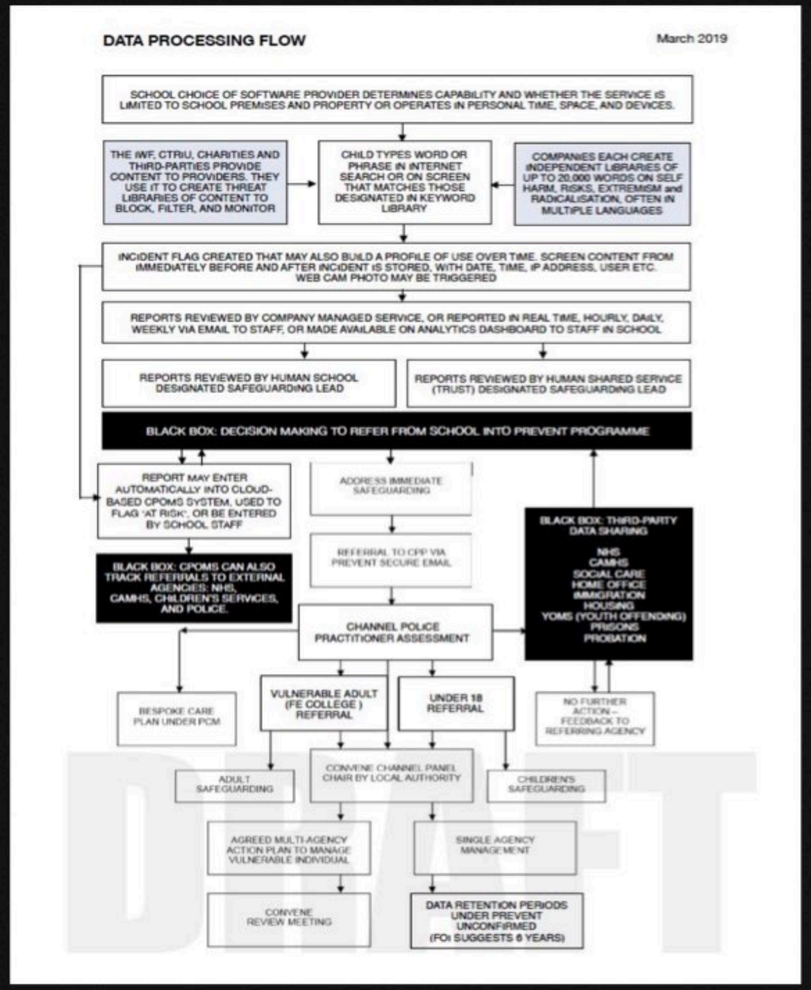
Date: _____

[1] Data Privacy and Security website: http://www.montgomeryschoolsmd.org/data-privacy-security/

1

What do you tell your pupils and why?

What does your classroom management software do?



DATA PROCESSING FLOW

March 2019

SCHOOL CHOICE OF SOFTWARE PROVIDER DETERMINES CAPABILITY AND WHETHER THE SERVICE IS LIMITED TO SCHOOL PREMISES AND PROPERTY OR OPERATES IN PERSONAL TIME, SPACE, AND DEVICES.

THE IWF, CTRIU, CHARITIES AND THIRD-PARTIES PROVIDE CONTENT TO PROVIDERS. THEY USE IT TO CREATE THREAT LIBRARIES OF CONTENT TO BLOCK, FILTER, AND MONITOR

CHILD TYPES WORD OR PHRASE IN INTERNET SEARCH OR ON SCREEN THAT MATCHES THOSE DESIGNATED IN KEYWORD LIBRARY

COMPANIES EACH CREATE INDEPENDENT LIBRARIES OF UP TO 20,000 WORDS ON SELF HARM, RISKS, EXTREMISM and RADICALISATION, OFTEN IN MULTIPLE LANGUAGES

INCIDENT FLAG CREATED THAT MAY ALSO BUILD A PROFILE OF USE OVER TIME. SCREEN CONTENT FROM IMMEDIATELY BEFORE AND AFTER INCIDENT IS STORED, WITH DATE, TIME, IP ADDRESS, USER ETC. WEB CAM PHOTO MAY BE TRIGGERED

REPORTS REVIEWED BY COMPANY MANAGED SERVICE, OR REPORTED IN REAL TIME, HOURLY, DAILY, WEEKLY VIA EMAIL TO STAFF, OR MADE AVAILABLE ON ANALYTICS DASHBOARD TO STAFF IN SCHOOL

REPORTS REVIEWED BY HUMAN SCHOOL DESIGNATED SAFEGUARDING LEAD

REPORTS REVIEWED BY HUMAN SHARED SERVICE (TRUST) DESIGNATED SAFEGUARDING LEAD

BLACK BOX: DECISION MAKING TO REFER FROM SCHOOL INTO PREVENT PROGRAMME

REPORT MAY ENTER AUTOMATICALLY INTO CLOUD-BASED CPOMS SYSTEM, USED TO FLAG 'AT RISK', OR BE ENTERED BY SCHOOL STAFF

ADDRESS IMMEDIATE SAFEGUARDING

BLACK BOX: THIRD-PARTY DATA SHARING

NHS
CAMHS
SOCIAL CARE
HOME OFFICE
IMMIGRATION
HOUSING
YOMS (YOUTH OFFENDING)
PRISONS
PROBATION

BLACK BOX: CPOMS CAN ALSO TRACK REFERRALS TO EXTERNAL AGENCIES: NHS, CAMHS, CHILDREN'S SERVICES, AND POLICE

REFERRAL TO CPP VIA PREVENT SECURE EMAIL

CHANNEL POLICE PRACTITIONER ASSESSMENT

BESPOKE CARE PLAN UNDER PCM

VULNERABLE ADULT (FE COLLEGE) REFERRAL

UNDER 18 REFERRAL

NO FURTHER ACTION – FEEDBACK TO REFERRING AGENCY

ADULT SAFEGUARDING

CONVENE CHANNEL PANEL CHAIR BY LOCAL AUTHORITY

CHILDREN'S SAFEGUARDING

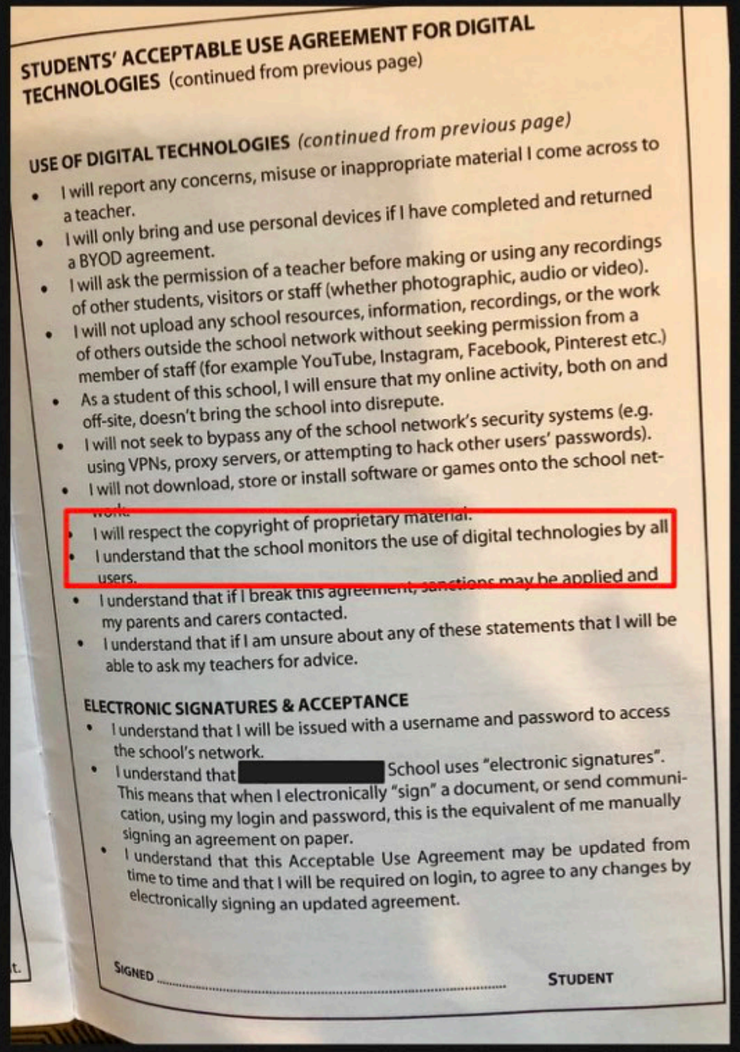
AGREED MULTI-AGENCY ACTION PLAN TO MANAGE VULNERABLE INDIVIDUAL

SINGLE AGENCY MANAGEMENT

CONVENE REVIEW MEETING

DATA RETENTION PERIODS UNDER PREVENT UNCONFIRMED (FOI SUGGESTS 6 YEARS)

DRAFT



STUDENTS' ACCEPTABLE USE AGREEMENT FOR DIGITAL TECHNOLOGIES (continued from previous page)

USE OF DIGITAL TECHNOLOGIES *(continued from previous page)*

- I will report any concerns, misuse or inappropriate material I come across to a teacher.
- I will only bring and use personal devices if I have completed and returned a BYOD agreement.
- I will ask the permission of a teacher before making or using any recordings of other students, visitors or staff (whether photographic, audio or video).
- I will not upload any school resources, information, recordings, or the work of others outside the school network without seeking permission from a member of staff (for example YouTube, Instagram, Facebook, Pinterest etc.)
- As a student of this school, I will ensure that my online activity, both on and off-site, doesn't bring the school into disrepute.
- I will not seek to bypass any of the school network's security systems (e.g. using VPNs, proxy servers, or attempting to hack other users' passwords).
- I will not download, store or install software or games onto the school network.
- I will respect the copyright of proprietary material.
- I understand that the school monitors the use of digital technologies by all users.
- I understand that if I break this agreement, sanctions may be applied and my parents and carers contacted.
- I understand that if I am unsure about any of these statements that I will be able to ask my teachers for advice.

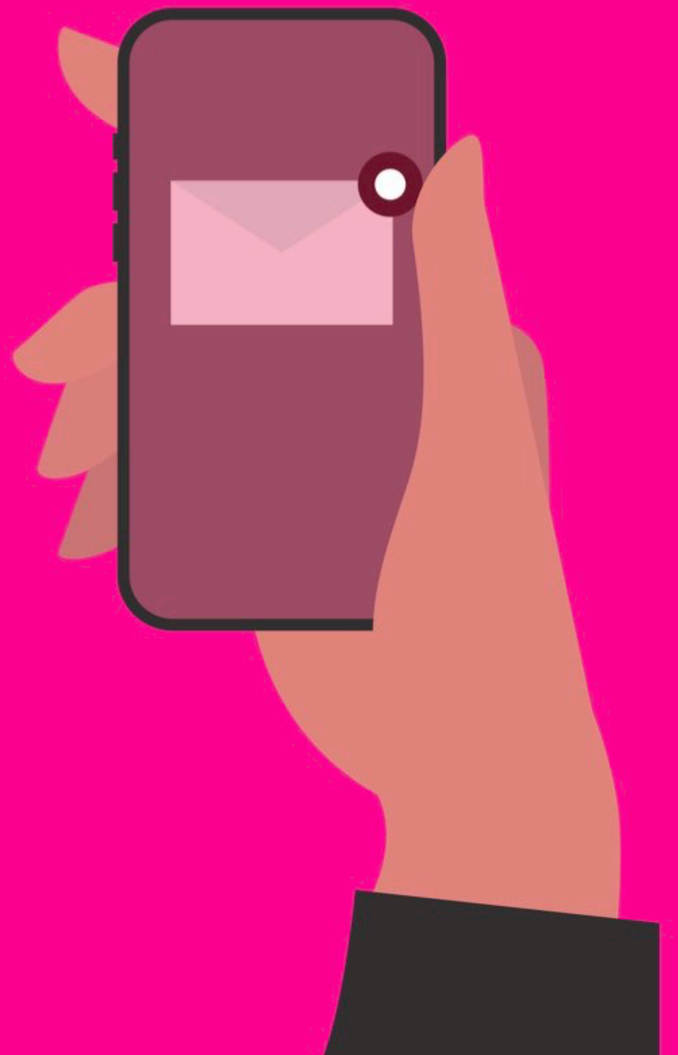
ELECTRONIC SIGNATURES & ACCEPTANCE

- I understand that I will be issued with a username and password to access the school's network.
- I understand that [redacted] School uses "electronic signatures". This means that when I electronically "sign" a document, or send communication, using my login and password, this is the equivalent of me manually signing an agreement on paper.
- I understand that this Acceptable Use Agreement may be updated from time to time and that I will be required on login, to agree to any changes by electronically signing an updated agreement.

SIGNED ..... STUDENT

“the price of innovation does not need to be the erosion of fundamental privacy rights.”

Elizabeth Denham, ICO, 3 July 2017,
findings on Google DeepMind and Royal Free Hospital unlawful processing of health data for the company’s product development

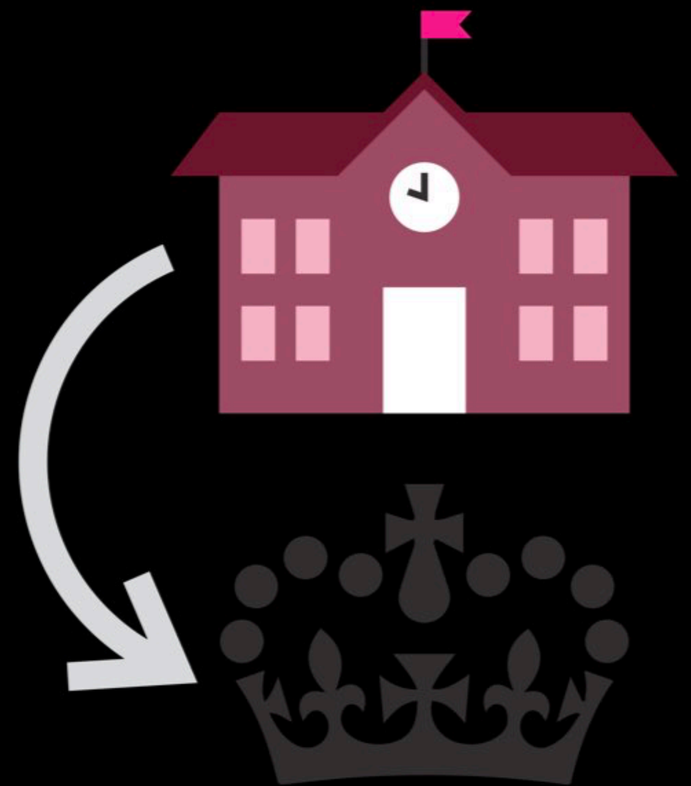


“Consent and contract terms must be rethought in the context of education.”

defenddigitalme, 2019

Recommendations for radical reform to deliver a rights-respecting digital environment in schools

- Reducing the investigative burden
- On children's agency
- The role of families
- The role of school staff
- A model management framework not consent
- Procurement
- Automated decisions, profiling, and AI
- Horizon scanning on new technology
- On the permanent single record
- Representation and remedy
- Data cycle lifetime accountability



And finally

Please register and remember to vote

@defenddigitalme

@TheABB

jen@defenddigitalme.com

defenddigitalme.com

Appendix for post event reference

Some of the US laws passed in last 5 years

- Arizona: For school districts that release directory information to educational and occupational/military recruiters, they must provide students with the opportunity to opt-out of that release.
- Arizona: Student transcripts can't be released unless the student consents in writing.
- Arizona: Ban on targeted advertising, using information to create profiles about students, sell or rent student's information, or disclose covered information.
- Arkansas: Ban on the state board or the state Dept. of Ed. from providing access of any student personal data collected at the state level to the federal Dept. of Ed or any Dept. of Ed program, nor their TA providers, research partners, government assistance organizations, or program monitors without parental consent.
- California: information can only be collected, used, and retained to administer the public services or programs for which that information was collected or obtained.
- Colorado: Prohibits collection of health records and biometric information and limits transfer of student data.
- Florida: Requires State Board to annually notify parents and students of their FERPA rights. Prohibits collection or retention of information such as political and religious affiliation, voting history, or biometric information of student, sibling, or parent. Prohibits use of a student's SSN as their identification number.
- Maryland: Longitudinal Data System shall be limited to no longer than 20 years from the date of latest attendance in any educational institution in the State.
- Montana: provisions apply to the purchase, merger, or other acquisition of an operator by another entity.
- Oregon: allow parents "the right to limit the collection, storage, use and transmittal of academic information and personally identifiable data." Would allow parents to opt-out of statewide summative assessments.
- Virginia: prevent a school service provider from using data for behaviorally targeting advertisements to students