Data Protection and Digital Information Bill

Second Reading briefing September 2022

About defend digital me

defenddigitalme is a call to action to protect children's rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. For more information see https://defenddigitalme.org/about/

defend|digital|me

Data Protection and Digital Information Bill

Second Reading briefing September 2022

Current data protection law fails to protect children from misuse of their personal confidential data in the education sector and children's social care – at national, and regional and at local levels.

1. What can you make better through this Bill?

1.1. Do you expect your children's identifying, personal confidential data including date of birth and home address, special educational needs and disability, attainment and grades, indicators for adoption or child-in-need or family in the armed forces, to be given away in bulk to businesses and the media, charities, think tanks or academic researchers simply as a result of going to school? If not, you have an opportunity in this Bill to change current practice for over 21 million people.

1.2. Do you accept that children in social care should be put at risk from automated systems about which world leading researchers at the Turing Institute have said, "*system errors, unreliable performance, and lurking biases may have life and death consequences.*"[1] If not, you have an opportunity to change current practice for thousands of children-at-risk, through this Bill.

1.3. Do you expect details of students' sexual orientation and religion collected as part of equality monitoring to be recorded against individuals' names in national databases and passed around other government bodies?If not, you have an opportunity to change this current practice for over 4 million Higher Education students in this Bill.

1.4. Do you believe organisations at growing risks from ransomware, hacking, data theft and security breaches should be doing <u>less</u> to protect people whose data they handle? If not, you have an opportunity to change this by not allowing the weakening of organisational accountability and due diligence that this Bill proposes and that will affect every educational setting across the UK.

1.5. Do you want to build a better safer environment for children in education free from exploitation of their confidential data without their consent? Then you have a chance to build better in this Bill through the appointment of a National Data Guardian for Education and Children's Social Care, and creation of a Code of Practice for data processing for children in education.

[1] Leslie, D. et al. (2020) *Ethics Review of Machine Learning in Children's Social Care.* The Alan Turing Institute and Rees Centre, University of Oxford, and WWCSC, (p51) https://whatworks-csc.org.uk/wp-content/uploads/WWCSC_Ethics_of_Machine_Learning_in_CSC_Jan2020_Accessible.pdf

2. How can you change this in the Bill?

2.1 In Part one, remove clause 5 (Bill pages 5-6).
This will create a new exemption from high standards of protection, if the proposed creation of conditions for processing for new legitimate interests goes ahead; in particular for safeguarding vulnerable individuals, which is a completely unnecessary change and will create a higher risk environment for individuals, not better practice.

2.2 Remove related Schedule one, Annex 1.
The insufficiently defined broad legitimate interests that would still be high risk, but not require risk assessment, should be removed. Such sensitive data processing does not need less attention or care. The protections are there to work for people, and create no barriers to good data practice. Reducing protections and due diligence creates risk.

2.3 In Part one, 50C(2) the measures for safeguards for automated decision-making (p.19)
This must not be weakened. Instead the public needs a transparency duty on public authorities to publish a register of risk assessments alongside algorithmic processing and automated decision-making. A plain English documentation of the algorithm would provide information about the data and processes available and publish information about how data are collected, secured and stored, as done through the Algorithm Charter for New Zealand.[2]

2.4 Remove Part one, clause 9(2) Information to be provided to data subjects. **(removal of obligation to tell people how their data is being processed in ways they do not expect or would object to – this is not applicable to things like criminal investigations.)**
This would allow data processing to proceed to which people may object because they would never be informed about it and unable to object, regards, "*information to be provided where personal data has not been obtained from the data subject"*. A real-life scenario is schools passing data to the Department for Education in the termly school census. It is wrong that the Secretary of State can simply decide, without notification to individuals, that "the controller intends to further process the personal data", and so their personal confidential data can be used for anything at all, in ways that people do not support, without telling them or giving them an opportunity to refuse. For example it could mean personal confidential data re-used to support the development of autonomous weapons, medical procedures that they disagree with on conscientious grounds, or simply for-profit use.

> *(f) the obligation referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the processing for which the personal data are intended.*

Many people would object to the objectives to commercialise school children's personal confidential records but they were not informed or given a choice in 2012. At that time

[2] The Algorithm charter for Aotearoa New Zealand demonstrates a commitment to ensuring New Zealanders have confidence in how government agencies use algorithms https://data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/

15 million named records were retained at the DfE and it increases with every new school intake each year. Now over 21 million named records are given away each year and no one has told the children, many now adults (anyone in England, state educated since 1996, as well as the exam results of those privately educated, which will include many MPs own personal data and their children or grandchildren's).

2.5 Support a new clause to notify and obtain consent before processing pupil information for commercial re-use by the Secretary of State.

2.6 Support a new clause to introduce the appointment of a National Data Guardian for Education and Children's Social Care (The DfE joint remit).

2.7 Support a new clause to create a Code of Practice around the safe and transparent processing of national pupil records from the Department for Education.

---

3. Parents don't know that pupil data is given away to companies for commercial re-use by the national government

We polled 1,004 families through Survation in 2018.[3] Nearly three-quarters had never heard of the National Pupil Database and did not know that their child's or their own personal confidential data was given away. The majority of parents (69%) polled said they had not been informed that the Department for Education may give their child's information to third parties.

When it comes to children with special educational needs or a disability, as many as 81% of parents said that parental consent should be required to share this data with third parties such as researchers and commercial companies..

Over 60% wanted parental consent to be required in order to pass this information on. Two in three said that parental consent should be required to pass data from schools to third-party *commercial* companies. We did not ask if they would prefer to not have it passed on at all.

Almost 4 in 5 (79%) said, if they had the opportunity, they would choose to see their child's named record in the Database (which today is not offered to families).

The proposals to change the UK Data Protection Act only four years after it first came into law will make things worse for school children. What changes might it make compared with the law as it stands today?

A new pro-growth data protection framework that "reduces burdens on businesses and boosts the economy" should not mean de facto that children should be exploited or accept infringement of their rights. The Data Protection Act has offered pupils limited

[3] Survation conducted the survey of 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme between 17th-20th February 2018.
https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

meaningful protection so far, and is about to get weaker. Lawmaking and procurement, policy and practice, must instead respect the UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.[4]

In summary, the planned reforms will undermine children's protection in law. This is not "data a new direction" but will amplify more of the same bad practices of today, heading in the wrong direction to defend children's right to privacy, identity, and security.

For children the costs of taking this wrong direction, may last a lifetime. It will have long-term consequences for national as well as individual security. The costs of this short term 'fast buck' approach will be borne not only by individuals, but by business and the research community through a loss of public trust in their data handling as risk is increased through more focus on data transfers abroad and treating people as the product.[5]

Instead, as we concluded in our report last year, *The words we use in data policy: putting people back in the picture (2021)*, "*we must reconcile the focus of the UK national data strategy, with a rights-based governance framework to move forward the conversation in ways that work for the economy and research, and with the human flourishing of our future generations at its heart.*" And young people must have agency in determining the use of data about them and feel in control of the stories of their lives[6].

Children and young people make up approximately a fifth of the population. Yet the lack of children and young people's voice in and about official statistics is a significant weakness,[7] according to the UK Office for Statistics Regulation.

---

4. Comment on the Bill Impact Assessment

4.1 Page 134 Clause 447(b) of the Bill Impact Assessment[8] (06/07/2022) suggests removing the duty on data processors to assess risk to rights and harms to the people involved whose data they are about to process. The proposals mean more is wrapped into broad and loose, 'legitimate interests'. The scenarios involved for children are among those where the *most* not the *least* care is needed, namely children's social care. It is fraudulent of the proposals to suggest that there will be

[4] General Comment No. 16 (2013) on State obligations regarding the impact of business on children's rights https://resourcecentre.savethechildren.net/library/general-comment-no-16-2013-state-obligations-regarding-impact-business-childrens-rights
[5] Global data experts fire up government's plans to promote free flow of data https://www.gov.uk/government/news/global-data-experts-fire-up-governments-plans-to-promote-free-flow-of-data
[6] The Words we use in data policy: young people's views (2021) defenddigitalme https://defenddigitalme.org/research/words-data-policy/
[7] Visibility, Vulnerability and Voice: The importance of including children and young people in official statistics. (2022.). *Office for Statistics Regulation*. https://osr.statisticsauthority.gov.uk/publication/visibility-vulnerability-and-voice-the-importance-of-including-children-and-young-people-in-official-statistics/
[8] Bill Impact Assessment 06/07/2022 https://publications.parliament.uk/pa/bills/cbill/58-03/0143/Data%20Protection%20and%20Digital%20Information%20Bill%20Impact%20Assessment%20-%20Final%20submission.pdf

benefits to children if there is weakening of what can be done with data about them under 'legitimate interests.'

In 2014 it was made explicitly clear in the Working Party 29 Opinion that, *"Article 7(f) [legitimate interests] should not become an easy way out from compliance with data protection law*." This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions, but this Bill makes no such strict definitions and instead proposes loose, broadly drawn conditions. The new conditions for legitimate interests are unnecessary and such deviations not in line with the GDPR, could jeopardise adequacy. The balancing tests must be kept.

4.2 Page 136 Clause 447(h) of the Bill Impact Assessment[9] (06/07/2022) states the removal of requirements to complete Data Protection Impact Assessments (DPIAs) could create detrimental effects of the processing for individuals. This is correct.

It fails to recognise however that such risk assessment is as much *a protection for the organisation* to be able to identify its own risks and mitigations, including reputational risks, as for *individuals*. For example, the DfE had failed to carry out risk assessments on national pupil data processing before it began which, if done properly would have better protected the Department.

The 2013 General Comment No. 16 on State obligations regarding the impact of business on children's rights paragraph 62, affirms the importance of risk assessment. *"Where there is a high risk of business enterprises being involved in violations of children's rights because of the nature of their operations or their operating contexts, States should require a stricter process of due diligence and an effective monitoring system.*" The DPIA duty must be kept in full and unaltered. For reference it is not burdensome in the 2018 UK Data Protection Act[10] as set out simply in current law:

" 64 Data protection impact assessment

(1)Where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2)A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3)A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;
(b) an assessment of the risks to the rights and freedoms of data subjects;
(c) the measures envisaged to address those risks;
(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing."

[9] Bill Impact Assessment 06/07/2022
https://publications.parliament.uk/pa/bills/cbill/58-03/0143/Data%20Protection%20and%20Digital%20Information%20Bill%20Impact%20Assessment%20-%20Final%20submission.pdf
[10] UK Data Protection Act 2018 c.12 Part 3 Chapter 4 General obligations section 64
https://www.legislation.gov.uk/ukpga/2018/12/section/64

4.3 Page 134 Clause 447(g) Future-proofing article 22 – protections for people from automated decision making – must be upheld. While the case study cited is exams 2020, the sensitivity of where automated decisions should not be underestimated and may apply in life-and-death situations such as children's social care. In September 2020, the *What Works for Children's Social Care* published a research report, in follow up to their earlier *Ethics Review of Machine Learning in Children's Social Care.* (see footnote 1). After working with four local authorities, and analysing thousands of case notes relating to tens of thousands of children, they tried to make a series of predictions about their future. "*What we find is not encouraging*," they wrote. *"Across 32 models, none meet the threshold we set in advance for success, with most of them falling far short of it. Models that attempt to predict the future – i.e. those that are actually useful in practice – do even worse – meaning that more families could see unnecessary intervention in their lives, and more opportunities for support could be missed."*

Why are such risky and unevidenced tools deployed in children's social care at all? Is the government going to wait until the 'life and death consequences' affect a child before they act to protect children from bad automated decisions that reduce or remove the humanity and accountability from the systems and institutions that need it most?[11]

4.4 Page 14 comments on Subject access requests (SARs) appear to suggest that people should not be allowed to know what goes on with our personal confidential data while businesses and others should be permitted to exploit information about us at will. The process is not complicated. Tell me what you process, how and why and give me a copy so that I can verify its accuracy. The Department for Education currently has a simpler process for press and companies to access children's identifying and sensitive records, than their own parents. Should this process be weakened or improved? Note that there has been no consultation undertaken with children in the Bill preparations.

---

5. Background: National pupil data processing since 1996

The Department for Education ("DfE") does not comply with the UK Data Protection Act 2018 according to an ICO audit, and does not meet the required standards of national pupil data processing for over 21 million name records in the National Pupil Database ("NPD"). The DfE started amassing detailed personal confidential data about school children and students over 20 years ago[12] and it is all given away. New safeguards are needed to protect children and learners.

Just over two years ago, the ICO completed an audit of the Department for Education.[13] A total of 139 recommendations for improvement were found, with over 60% classified as urgent or high priority.

---

[11] Blog : Artificial Intelligence in Children's Social Care. https://defenddigitalme.org/2022/03/15/world-social-work-day-2022-artificial-intelligence-in-csc/

[12] Defend Digital Me Pupil data 20 years on https://defenddigitalme.org/2022/01/04/20-years-on-childrens-names-in-national-pupil-data/

[13] Copy of the ICO executive summary of the DfE audit (2020) https://defenddigitalme.org/wp-content/uploads/2021/10/department-for-education-audit-executive-summary-marked-up-by-DDM-Jan-2021.pdf

- “The DfE cannot demonstrate accountability to the GDPR”
- “The DfE are not providing sufficient privacy information to data subjects as required by Articles 12, 13 and 14 of the GDPR.”
- “The DfE are not fulfilling the first principle of the GDPR, outlined in Article 5(l)(a), that data shall be processed lawfully, fairly and in a transparent manner.”
- “The lack of awareness amongst staff presents a high risk that data will not be processed in a compliant manner and could result in multiple data breaches or further breaches of legislation.”
- “The Commercial department do not have appropriate controls in place to protect personal data being processed on behalf of the DfE by data processors.”
- “there is limited oversight and consistency around how data is shared externally”.

The NPD is now “one of the richest education datasets in the world,” holding a wide range of highly sensitive information about pupils and students dating back to 1996 including indicators of children at risk, adoption and fostering flags. Named records are retained indefinitely, long after children leave school, and the ICO audit raised lack of weeding or disposal as an issue. Between March 2012 to June 2021 we have calculated there have been over 2,000 releases containing sensitive, personal or confidential data at pupil level, each release of millions of records but the Department cannot even tell you which of its third-parties were given your child’s identifying records. Not anonymous.

The promise twenty years ago that names would only be used for statistics was broken. Ten years ago Michael Gove said, “*Organisations granted access would need to…fully protect the identity of individuals.*” Identifying data has been given away since 2012. Even gambling companies were using information obtained via a third-party with access to the DfE Learner Records Service, to onboard new customers in 2020.[14]

Today, pupil data is given away by the million in identifying and sensitive form. Instead, the recommendations in the 2018 International Conference of Data Protection and Privacy Commissioners resolution on e-learning platforms,[15] should be broadly applied as the basis of a Code of Practice for pupil data processing in UK education.

It is well evidenced from over a decade of public engagement that people want control over what is done with data about them.

In December 2018, UCL researchers[16] “carried out a public engagement session with a group of Young Research Advisors (ten young people aged 9 to 24 years from primary school to post-university) facilitated by the National Children’s Bureau on the topic of data sharing involving the NPD and health data. Participants were supportive of anonymous data sharing for research (including the sharing of identifiers for linkage through a third party model) providing sufficient safeguards are in place. The group also recognised the potential benefits of sharing data between services to support individual decision-making. **However, the need for individual consent was highlighted, as was the suggestion that data flows from health to education would require more stringent safeguards, rather than the other way around.”**

---

[14] BBC The Papers (January 2020) https://youtu.be/Y8a-S7LGvL8 Betting firms use data from Department for Education Learner Records Service

[15] ICDPPC Resolution on E-Learning Platforms (40th International Conference of Data Protection and Privacy Commissioners (October 2018) https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

[16] UCL on the Data Resource: the National Pupil Database (NPD) https://ijpds.org/article/view/1101

There is no public support for reducing everyone's data protection rights.
In the British student population, one 2015 survey of university applicants in England, found of 37,000 who responded, the vast majority of UCAS applicants[17] agree that sharing personal data can benefit them and support public benefit research into university admissions, but they want to stay firmly in control. 90% of respondents said they wanted to be asked for their consent before their personal data is provided outside of the Higher Education admissions' service.

A 2014 survey for the Royal Statistical Society by Ipsos MORI, found that trust in institutions to use data is much lower than trust in them in general.[18]

In 2010, a multi method model of research with young people aged 14-18, by the Royal Society of Engineering, found that, "*despite their openness to social networking, the Facebook generation have real concerns about the privacy of their medical records.*" [2010, Privacy and Prejudice, RAE, Wellcome][19]

---

6. Local pupil data processing in education

6.1 Multiple schools across the UK regularly lose sensitive personal confidential pupil data as a result of poor security susceptible to ransomware attacks (2022)

In the most recent public case in the media, hackers stole private data including children's passports, sensitive and detailed disciplinary records, and child protection reports relating to vulnerable pupils from schools.[20] The leak included a list of students excluded from St Paul's Catholic College in Sunbury-on-Thames, Surrey. Stolen pupil data was also leaked from the De Montfort School, Evesham, Worcestershire, and Carmel College, St Helens, Merseyside, Pilton Community College in Barnstaple, Devon, and Mossbourne Federation in Hackney, London.

6.2 Barnsley (2018) Pupils with special educational needs confidentiality breach

Human error can erode trust and damage the likelihood of future cooperation with councils. In 2018, a Barnsley council error meant the personal details of parents of children with special educational needs were sent out to hundreds of people.*"Parents have said to the council 'good luck on us filling anything out again'."*[21]

[17] UCAS survey (2015) https://www.ucas.com/file/36556/download?token=lvGg2GQe
[18] New research finds data trust deficit with lessons for policymakers. (2014). Ipsos. https://www.ipsos.com/en-uk/new-research-finds-data-trust-deficit-lessons-policymakers
[19] Young people's views on the development and use of Electronic Patient Records (2010) https://raeng.org.uk/media/cydjha4a/privacy_and_prejudice.pdf
[20] Daily Mail (2022) Thousands of children at risk from grooming gangs as hackers leak their private details https://www.dailymail.co.uk/news/article-10976707/Hackers-leak-private-data-thousands-children-dark-web.html
[21] Barnsley Chronicle (2018) Full investigation promised after data breach https://www.barnsleychronicle.com/article/13125/full-investigation-promised-after-data-breach

6.3 Biometric pupil data processing

We completed research on UK children and biometric data in May 2022[22]. Ten years after the adoption of the UK Protection of Freedoms Act 2012 we find that it and current UK Data Protection law are not enough to protect children's rights in educational settings. Emerging harms and scope creep have advanced since they were written, particularly around the use cases in education such as claims around using artificial intelligence for emotion detection and tools designed to affect mood or influence mental health that sit outside the narrow definition of biometrics for ID purposes.

Some schools **discriminate against children in receipt of Free School Meals** by making it seem obligatory for pupils who qualify for FSM to be signed up to the biometric system in order to continue to receive their lunch, while other pupils can choose not to use it.[23] This is in breach of the law. While cashless payment systems may be made obligatory, using them with a PIN or card must also be possible. Offering only biometrics is in breach of the Protection of Freedoms Act 2012.

Already in 2018, on our behalf, Survation polled 1,004 parents of children in state schools about their experience of technology in schools. Despite the law demanding parental consent an obligation, 38% of parents whose children were using biometrics in school, said they had not been offered any choice, and over 50% had not been informed how long the fingerprints or other biometric data is retained for, or when they will be destroyed.

Despite being found unlawful and since removed from schools in France, Sweden and parts of the U.S., facial recognition is growing across UK schools. There is widespread recognition of research evidence that facial detection, facial recognition and biometric systems are discriminatory. In 2019, researchers for the U.S Department of Commerce National Institute of Standards and Technology (NIST) found, “elevated false positives in the elderly and in children; the effects were larger in the oldest adults and youngest children, and smallest in middle aged adults.”

> “children… are disadvantaged …by being excluded by policy, or by encountering higher false negatives. Age itself is a demographic factor as accuracy in the elderly and the young differ for face recognition (usually) and also for fingerprint authentication. This applies even without significant time lapse between two photographs.”[24]

On gender and race they concluded that Buolamwini and Gebru’s 2018 research found some facial analysis algorithms misclassified Black women nearly 35 percent of the time, while nearly always getting it right for white men.

---

[22] The State of Biometrics 2022: A Review of Policy and Practice in UK Education https://defenddigitalme.org/research/state-biometrics-2022/

[23] “*Accounts must be topped up in advance using the ParentPay system and this can be done either online or via a PayPoint. Students who qualify for FSM will need to be signed up to the biometric system in order to continue to receive their lunch.*” https://www.buxtonschool.org.uk/542/biometric-system

[24] 2019 report for the U.S Department of Commerce National Institute of Standards and Technology (Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects) https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

6.4 House of Lords: Biometric Recognition Technologies in Schools, Nov. 4, 2021 Lord Scriven

"If we leave it to individual schools, the unintended consequences and problems that will arise will be not just technical but deeply ethical and societal. There must be a balanced debate within this Parliament and legislation must be brought forward. We have seen the unintended consequences in live facial recognition use by the police when the marketing teams and the technology gets ahead of the legislation. We talk then about the lack of regulation, rather than first talking about where it is acceptable and unacceptable and we start seeing that, as the technology leads, people's rights are trampled on and we try to play catch-up."

"This debate is very fundamental. It is a debate about where we, as a society, draw the line in the use of technology—not about what we do once it is deployed but what the limitations of it are before we start talking about how it is regulated. This cannot be left to individual schools or councils. It is for this Parliament to legislate and to decide where we draw that line."

6.5 Baroness Chisholm of Owlpen

"I cannot believe it will not be discussed at great length as far as legislation is concerned. All the concerns brought up today are very live and important and need a great deal of thought. I will take this back to the Department for Education, but it is the Department for Digital, Culture, Media and Sport which really needs to get involved in this. I think everyone is almost wondering what is coming next."

6.6 Scottish Parliament, October 2021

The MSP for North East Fife Willie Rennie asked what the Scottish government position is on facial recognition in schools on October 28th in the Scottish Parliament. The First Minister, Nicola Sturgeon, responded that she felt the technologies do not appear to be proportionate or necessary.

---

7. Where is the code of accreditation and what will it do?

In debate on the Post-16 education and Skills Bill, in October 2021, rather than proceed with safeguards written into the Bill in the form of an ICO Code of Practice on student data processing by the government and other public and arms length bodies, the government stated that a code of accreditation was in progress.[25]

It was claimed they were working on it with the ICO and that edTech companies would be written to by the end of the year (December 2021). In February Lord Scriven was told the work was completed, and it would be deposited in the HOL library by the end of March. It is yet to be seen or discussed in the public domain or to explain its scope..[26]

[25] Hansard Baroness Barran on Thursday 21 October 2021
https://hansard.parliament.uk/Lords/2021-10-21/debates/AE4D13AD-9A4A-46BE-A93C-2B739A49E020/SkillsAndPost-16EducationBill(HL)#contribution-9D45CF0F-29E9-4505-906E-B1BE07C0694A

[26] February 2022: Lord Scriven was told the work was complete and it would be deposited in the HOL library in March

8. Proposed amendments

8.1 Requirement to notify and obtain consent before processing pupil information for commercial re-use by the Secretary of State

New Clause insert—'.

Protection of pupil data

(1)This section applies in relation to any processing of a child's personal data by or on behalf of the relevant authority of—

(a) a school,
(b) a 16 to 19 Academy, or
(c) (c)a further education institution.

(2) Before the first processing of a child's personal data on or after the coming into force of subsection (3), the relevant authority must notify each parent of the child—

(a) of the Secretary of State intention to process the child's personal data, and

(b) that the parent may object at any time to the processing of the personal data for commercial purposes.

(3) The relevant authority must ensure that a child's personal data is not processed unless—

(a) at least one parent of the child consents to the information being processed, and

(b) no parent of the child has withdrawn his or her consent, or otherwise objected, to the information being processed.

(4) The relevant authority must make further provision about the requirement to notify parents and the obtaining and withdrawal of consent (including when notification and consent are not required).

(5) But if, at any time, the child—

(a) objects to the processing of that information,

the relevant authority must ensure that the information is not processed, irrespective of any consent given by a parent of the child under subsection (3).

---

https://questions-statements.parliament.uk/written-questions/detail/2022-02-09/HL6145/

8.2 National Data Guardian for Education and Children's Social Care

New Clause insert—'.

National Data Guardian for Education and Children's Social Care

1 National Data Guardian for Education and Children's Social Care

(1)The Secretary of State must appoint an individual to hold office as the National Data Guardian for Education and Children's Social Care (in this Act, "the Data Guardian").

(2)The Data Guardian may publish guidance about the processing of education and children's social care data in England.

(3)The following must have regard to such guidance—

(a)a public body exercising functions that relate to the education service, children's social care or child carer support in England;

(b) a person (other than a public body) providing—

(i) services as part of the education service,

(ii) children's social care, or

(iii) carer support,

pursuant to arrangements with a public body falling within paragraph (a).

(4) The Data Guardian must keep under review any guidance that has been published and has effect.

(5) The Data Guardian may revise any guidance as the Data Guardian considers appropriate, but if any guidance is revised, the guidance must be published as revised.

(6) Before publishing any guidance, the Data Guardian must consult such persons as the Data Guardian considers appropriate.

(7) The Data Guardian may give advice and information about, and assistance in relation to, the processing of education and children's social care data in England.

(8)The power to publish guidance or to give advice, information and assistance may (as well as being exercised in relation to all cases to which it extends) be exercised in relation to—

(a) those cases subject to specified exceptions, or
(b) particular cases or classes of case.

8.3 Create a Code of Practice around the processing of pupil data in education

New Clause insert—'.

Code of practice

(1) The Information Commissioner must issue a code of practice about—

(a) obligations and rights when processing personal information of parents and children under the Act by,

(i) educational settings

(ii) local education authorities and their further processors, and

(iii) disclosure to the Secretary of State, or any other prescribed person under the Education Act 1996,

(b) the right of parents and children to make a Subject Access Request without charge in order to receive a copy and validate the accuracy of their own personal data held by the Secretary of State, and to request correction of inaccuracies,

(c) the rights of parents and children in regards to automated decision-making and profiling,

(d) the nature and frequency of data processing demands by a public authority,

(e) an obligation on public authorities to publish statistics and records of pupil data processing on an annual basis, including a register of risk assessments and algorithmic processing,

(f) routes for complaint and redress.

(2) The code of practice must be consistent with the code of practice prepared under section 121 of the Data Protection Act 2018 (data-sharing code) and issued under section 125(4) of that Act] (as altered or replaced from time to time).

(3) A public authority must have regard to the code of practice in processing and disclosing personal information.

(4) A data processor or data controller must have regard to the code of practice for the processing of information under the Act by any person who is accredited under—

(a) section 71(1)(a) of the Digital Economy Act 2017; or
(b) any prescribed person under the Education Act 1996; or
(c) the Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009; or
(d) any other person.

(5) The Information Commissioner may from time to time revise and re-issue the code of practice after consultation with—

(a) the Minister for the Department for Education,

(b) the Statistics Board,
(c) the Ministers from Northern Ireland, Scotland and Wales,
(d) organisations that represent the interests of children and families and such other persons as The Information Commissioner considers appropriate.

(6) The Information Commissioner may not issue the code of practice unless a draft of the code has been laid before, and approved by a resolution of, each House of Parliament.

(7) In disclosing information, a person must have regard to the further codes of practice issued by the Information Commissioner under section 128 of the Data Protection Act 2018 (other codes of practice), so far as they apply to the information in question—

(a) any code which makes provision about the identification and reduction of the risks to privacy of a proposal to disclose information;
(b) any code which makes provision about the information to be provided to data subjects (within the meaning of that Act) about the use to be made of information collected from them.

---

defend|digital|me