defenddigitalme Response to the ICO consultation on FOI

March 2019

I. RESPONSE TO THE ICO CONSULTATION QUESTIONS **2**

1. Goal one. Improve standards of accountability, openness and transparency in a digital age
   a. Case study: Exam boards in England
   b. Case study: Integrated Dataset: children and young people (Bristol)

2. Goal three. Raise awareness of access to information rights and make them more accessible 3
   a. Case study: Using Freedom of Information law to uncover schoolchildren's data used to support the Hostile Environment

3. Goal four. Promote the reform of information rights legislation to remain fit for purpose 4
   a. Case study: transparency and accountability for data processing by Children's Safeguarding Boards and Multi Agency Safeguarding Hubs (MASH) 5
   b. Diagram: Data flows about children processed into, across and out of Prevent 7

II. CIVIL LIBERTIES GROUPS SHARED CONCERNS FOR CHILDREN AND FOI **8**

1. A chronic lack of transparency
2. What impact do you think our proposals will have on equality and human rights?

III. RECOMMENDATIONS **9**

1. Expansion
2. Enforcement
3. Education

I. Response to the ICO consultation questions

1. Goal one: Improve standards of accountability, openness and transparency in a digital age

We would welcome increased FOIA enforcement activity through targeting of systemic non-compliance, consistent with the approaches set out in the ICO Regulatory Action Policy.

We would support working in partnership with the ICO, and public authorities as part of civil society contributions, to research and promote new digital approaches to proactive disclosure of information, including making the most of open data opportunities.

One such opportunity is with Exam Boards, currently not subject to Freedom of information but which fail to provide adequate data in the public domain about data handling, and how they meet Data Protection Law.

A. Case study: Exam boards in England

In 2018 we asked seven exam boards in England via Freedom of Information requests[1], how they meet Subject Access obligations of the Data Protection Act 2018 (DPA2018) and for information about their data handling including foreign transfer, data retention, and use of automated decision making. These information are not made readily available to a candidate, and in our opinion fails to meet the obligations of the DPA2018 and GDPR, and fails obligations of accountability and transparency.

While some did provide limited information, or a link to a website, others refused.[2]

On March 6, 2019, Daniel Zeichner Member of Parliament for Cambridge, (15:06:35) pointed out in Parliamentary debate[3], on *Extending the Freedom of Information Act to housing associations and public contractors* that there is "a skewed playing field" since all bar the Cambridge exam board, are not subject to the Freedom of Information Act.

Enforcement of standards on Exam Boards should not be dependent upon the Freedom of Information Act, but we lack any ability to enforce such transparency, and total lack of accountability to children, young people and other students, who are subject to these business processes without any choice.

B. Case study: Integrated Dataset: children and young people (Bristol)

In 2018-19 we asked selected Local Authorities to provide a list of which datasets are linked with children's education records, at pupil level, since this is not available in the public domain or made actively open to schools.

Nearly 12,000 pupils' individual school records are extracted daily to a regional database and linked with a range of other data but which items are not public, or communicated to families.

We asked the Local Authority for this list, but the response has been delaying, and obtuse. This is an example of information that should be open data -- not the data from the individuals, but the list of data items to explain what is extracted.[4] Proactive disclosure of information, would support the duty under DPA 2018 that they currently fail to meet.

[1] FOI requests to Exam Boards via whatdotheyknow.com https://www.whatdotheyknow.com/info_request_batch/317
[2] Exam Boards: Subject Access Policy to Pearson EdExcel https://www.whatdotheyknow.com/request/exam_boards_subject_access_polic_2
[3] Parliamentary debate March 6, 2019 https://parliamentlive.tv/Event/Index/ea880651-a637-402c-8511-ce36b88a04f2
[4] FOI to Bristol City Council asking for a list of the data items by individual item, that may be included in the daily transfer https://www.whatdotheyknow.com/request/integrated_dataset_children_and_6

2. Goal three: Raise awareness of information rights and accessibility

The public has a Right to Know and should be encouraged to make use of their rights.

We welcome the recognition in the consultation that the ICO should understand different capability and needs among different groups of the population, to target awareness-raising and education efforts; and in particular that this approach, "*will also be reflected in the new Children's Strategy*".

However, this must be accompanied by stronger ICO enforcement of current failures of local authorities to be compliant with FOI timeliness, and inaccurate and over reliance on the application of exemptions. Otherwise increased awareness will only increase unmet demand.

Delays to provide information are used to impede public transparency and accountability of government policy, including in the formulation of new law. Where such policy goes otherwise without scrutiny or policy makers mislead the public, there needs to be a swift mechanism for early intervention.

We waited a year for the conclusion of enforcement of a Freedom of Information request in 2016, which had we had access to sooner, may have saved the public purse funding and public trust in policy makers, ahead of a drawn out failure of policy making that took over two years[5] to reach its conclusion, and caused gross interference with human rights in the process.

A. Case study: Using Freedom of Information law to uncover schoolchildren's data used to support the Hostile Environment [6]

When defenddigitalme challenged the Department for Education refusal in July 2016 to access meeting minutes of the Star Chamber Scrutiny Board (SCSB) about the decision to expand the school census that would begin in the following October, over a year's delay significantly impacted the ability to use that information to challenge the introduction of secondary legislation in July 2016, and use it in proceeding with judicial review in a timely manner, but it took too long to be able to enforce the DN.

The secondary legislation committee[7] did not have access to the full facts when it was deciding whether or not to review the introduction of the statutory instrument 808/2016 introduced and enacted within six weeks. Freedom of Information is a tool that enables retrospective scrutiny, when such policy changes are not subject to consultation or adequate legislative scrutiny.

Currently disclosure can be delayed without penalty, and delays become a vehicle to prevent scrutiny and in this case, harmed the just democratic process of lawmaking. To some extent, we agree with the Campaign for Freedom of Information when it says, "*The ICO has both informal and powerful formal tools for addressing persistent delays by public authorities, but is currently using neither."*[8]

While we supported the ICO in its successful enforcement of the Decision Notice in this case, it took far too long to reach conclusion, and became less useful as time went on.[9]

Due to delays to another FOI, Ministers were able to claim in parliamentary debate without evidence to challenge it, that "*These new data are solely for the DfE to use in research, statistics and analysis,*"[10]

[5] Schools Week, April 2018, DfE ends divisive pupil nationality data collection https://schoolsweek.co.uk/dfe-ends-divisive-pupil-nationality-data-collection/
[6] MySociety blog https://www.mysociety.org/2019/01/23/using-whatdotheyknow-to-uncover-how-schoolchildrens-data-was-used-to-support-the-hostile-environment/ See full timeline with links to relevant FOI requests at defenddigitalme https://defenddigitalme.com/timeline-school-census/
[7] Defenddigitalme letter to the SLSC
https://www.parliament.uk/documents/lords-committees/Secondary-Legislation-Scrutiny-Committee/Defenddigitalme-submission-SI2016-808.pdf
[8] Campaign for FOI https://www.cfoi.org.uk/2019/03/london-councils-foi-performance-assessed/
[9] School Census data expansion timeline with links to all relevant FOI https://defenddigitalme.com/timeline-school-census/
[10] School Census: Pupils' Nationality– in the House of Lords at 3:29 pm on 12/10/ 2016 https://www.theyworkforyou.com/lords/?id=2016-10-12b.1888.2

while we waited three months for the publication of a pre-existing data sharing agreement that showed the data would be handed over to the Home Office for the purposes of the Hostile Environment.[11]

In FOI request Ref: 2016-0032573[12] the Department for Education was able to withhold the full picture of facts, by minimising what it disclosed. For example, while revealing that data sharing from the 23 million records in the National Pupil Database[13] with the Home Office and Police had been taking place since April 2012, it said there had only been 18 data sharing requests.

The ***volume*** of each Home Office request, in those eighteen (monthly) requests, added up to over 2,500 individuals, and was only revealed later through a further FOI we made on October 27, 2016. Had we not pursued this, the original response would have been misleading.

FOI is a useful tool to increase openness of policy, not only on single occasions. The use of FOI quarterly to ask for these data sharing statistics, encouraged a change in policy so that numbers are now published quarterly. Such data and policy moved from secret, to open, as a result of FOI to include[14]:

- data shares with Home Office
- data shares with police and criminal investigation authorities
- data shares through court orders.

3. Goal four: Promote the reform of information rights legislation to remain fit for purpose

We would welcome recommendations for change, to build and promote the case for expansion of the scope of FOIA in relation to outsourced public services and some other categories of public service provision that are not within the scope of current legislation.

The Children's Commissioner report, *Who Knows What About Me,* published in November 2018 highlighted on children's data handling, that, "*public bodies do not always observe robust standards of privacy, transparency, security or redress.*"[15]

To oversee and enforce such standards in a timely manner is made more difficult where the activity is shared across a mixed set of providers, and responsibility is passed around or accountability is refused where bodies are not subject to FOI.

The outsourcing of services to the private sector has extended the number of bodies involved in state interventions and activity involving children often in multi-agency processes without extending suitable independent oversight and mechanisms for accountability and redress. Without Freedom of Information access rights to these mixed-function bodies, they remain opaque and unaccountable for public funding, secretive and untrustworthy to the individuals subject to their interventions, and are seen to be kafkaesque in their dealings with families.

Transparency and accountability are necessary to restore public trust in such extended networks of complex public sector and commercial interventions. We welcome the recognition in the ICO report that it is in the public interest that our access to information laws can be extended in proportionate ways and that Children's Safeguarding Boards are one of the key areas that should be addressed.[16]

[11] MOU between the Hoe Office and DfE in place from 2015 to October 2016 and then updated https://www.whatdotheyknow.com/request/377285/response/941438/attach/4/20151218%20DfE%20HO%20Final%20V0%201%20REDACTED.PDF.pdf
[12] FOI https://www.whatdotheyknow.com/request/pupil_data_sharing_with_the_poli#incoming-846569
[13] FOI to ask for basic information on the National Pupil Database not in the public domain at the time of asking 2015 https://www.whatdotheyknow.com/request/pupil_data_national_pupil_databa_2?
[14] DfE External Data Shares https://www.gov.uk/government/publications/dfe-external-data-shares
[15] Children's Commissioner report, Who Knows What ABout Me (2018) https://www.childrenscommissioner.gov.uk/2018/11/08/childrens-commissioners-report-calls-on-internet-giants-and-toy-manufacturers-to-be-transparent-about-collection-of-childrens-data/
[16] Outsourcing Oversight? The case for reforming access to information law p54 https://ico.org.uk/media/2614204/outsourcing-oversight-ico-report-to-parliament.pdf

A. Case study: transparency and accountability for data processing from children by Children's Safeguarding Boards and Multi agency safeguarding hubs (MASH)

Incidents recorded about a child in school can create triggers which start the child's entry into the Prevent programme through Children's Multi-Agency-Safeguarding-Hubs (MASH) and so-called, Channel Panels.

How or under which criteria data are shared, retained, action determined or decided against is opaque. Section 36 of the Counter-Terrorism and Security Act 2015 (CTSA) requires that this activity is done with the individual's consent. In reality, consent is coercive not freely given, or able to be easily refused.[17]

Referrals from schools feed into the Prevent programme via Channel,

> "*which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation*."

However, the scope creep since 2015 of this programme now means that the reasons ***why*** children may be referred under much broader safeguarding terms, radicalisation and extremism, have been expanded upon the previously more narrow lens of having capability and intent to terrorist action.

The drift in ***who*** can make referrals has changed very recently. The 2019 Counter Terrorism and Border Security Act newly enables Local Authorities to be able to refer an individual for discussion at a Channel panel.[18]

At the moment, this power is only available to the police. To achieve this change, the 2019 Act amends sections 36 and 38 of the Counter-Terrorism and Security Act 2015. This risks watering down the level of oversight applied in the process, from what the public expects exists within the police services to an unaccountable opaque Local Authority body.

So while the scope of children's involvement in such interventions has expanded, there has been no similar expansion of the accountability and transparency of the bodies involved, and their work of a public nature.

Concretely, we asked the Birmingham Safeguarding Children Board in late 2018 for information on the process. We were told instead to apply to ask Birmingham City Council. They replied to say they held the requested information, however, the Council refused saying it was exempt under section 24 (national security), 31 (law enforcement) and 38 (health and safety) of the Act. They then went on to suggest we asked the Birmingham Safeguarding Children Board, which falls under the Local Safeguarding Children Board Regulations 2006. The BSCB then replied to say, it was,

> "*a statutory body in its own right, distinct from Birmingham City Council and Birmingham Children's Trust. It is not a public authority for the purposes of the Freedom of Information Act 2000 (the Act), and is therefore not subject to requests for information under the Act.* ***The Information Commissioner's Office has previously considered this matter."***

The ICO Decision Notice[19] it applied was with regard to serious case reviews -- and in our opinion was misused to deny our request for very different information, including a copy of the board privacy notice and statistics.

All six Local Authority Safeguarding Boards and councils we asked, failed to provide the numbers of children referred which we wanted in order to ask schools in the area about the workings of the programme to scrutinise and uphold children's human rights. Our FOI to Local Authorities were refused on grounds of national security, and by Safeguarding Boards because they are not subject to FOI. They each used similar wording to refuse.

[17] Section 36 of the Counter-Terrorism and Security Act 2015 (CTSA) https://www.legislation.gov.uk/ukpga/2015/6/section/36
[18] https://defenddigitalme.com/wp-content/uploads/2019/03/2019-02-12_Channel_Panel_Fact_Sheet_RA.pdf
[19] ICO DN https://ico.org.uk/media/action-weve-taken/decision-notices/2011/639676/fs_50368110.pdf

Our Freedom of Information requests asked for the retention policy for data processing into, across and out of such panels. Article 5 (1)(e) of the GDPR and 5 (4)(e) of the Convention 108 require data to be kept in a form which permits identification of individuals [data subjects] for no longer than is necessary for the purposes for which the data are processed. The data must therefore be erased when those purposes have been met. Our research has found inconsistent data retention periods for records created from log files of web searches and screen content retention in schools used in such referrals, including data retention of 'indefinitely' until the customer [school] requests deletion, and retention in the US. We wish to scrutinise retention across the process.

Not only has the programme expanded in who and why children are involved over the last 5 years, but this increasingly involves private companies handling children's sensitive personal data, -- profiles containing or inferring mental health, suicide, self harm and radicalisation and terrorism content --, and information which the children may be unaware is captured by one of the many growing companies widespread in UK education.

Some of these companies are owned by private equity, are based in the Middle East or US without transparency of their operations and internal data handling processes. It is certainly not an interaction that parents expect of 8.2m children's data, when they send a child to a school every day in England. We carried out a survey of 1,004 parents of state educated children in 2018 and nearly 90% wanted more transparency of these processes.[20]

The accountability principle of GDPR Article 5 (2) is shared between controllers and processors. The Working Party 29 noted compliance mechanisms vary according to the severity of the risks and implications represented by data processing. But we cannot extend scrutiny aligned with this duty of accountability to both parties, where public obligations cross into the private sector because rather than applying private contractors rights, they claim commercial sensitivity exemptions.

The processing of information from children with such high risks of potential for stigma and discrimination could hardly be more sensitive. Yet there is no Code of Conduct or due diligence for the conduct of school staff or companies in this growing commercial sector of data processing, or due regard for the rights of the child under the UN Convention on the Rights of the Child and the Human Rights Act 1998.

Transparency and accountability are lacking at the highest levels for these policies, as much as across the public sector and commercial players for the processing in a manner compatible with human rights and data protection law. Without the scrutiny that FOI law supports, accountability is lacking and hard to challenge in order to protect the rights of the child. Children find it impossible to make such requests themselves, and are often unaware of such processing activities and their rights.

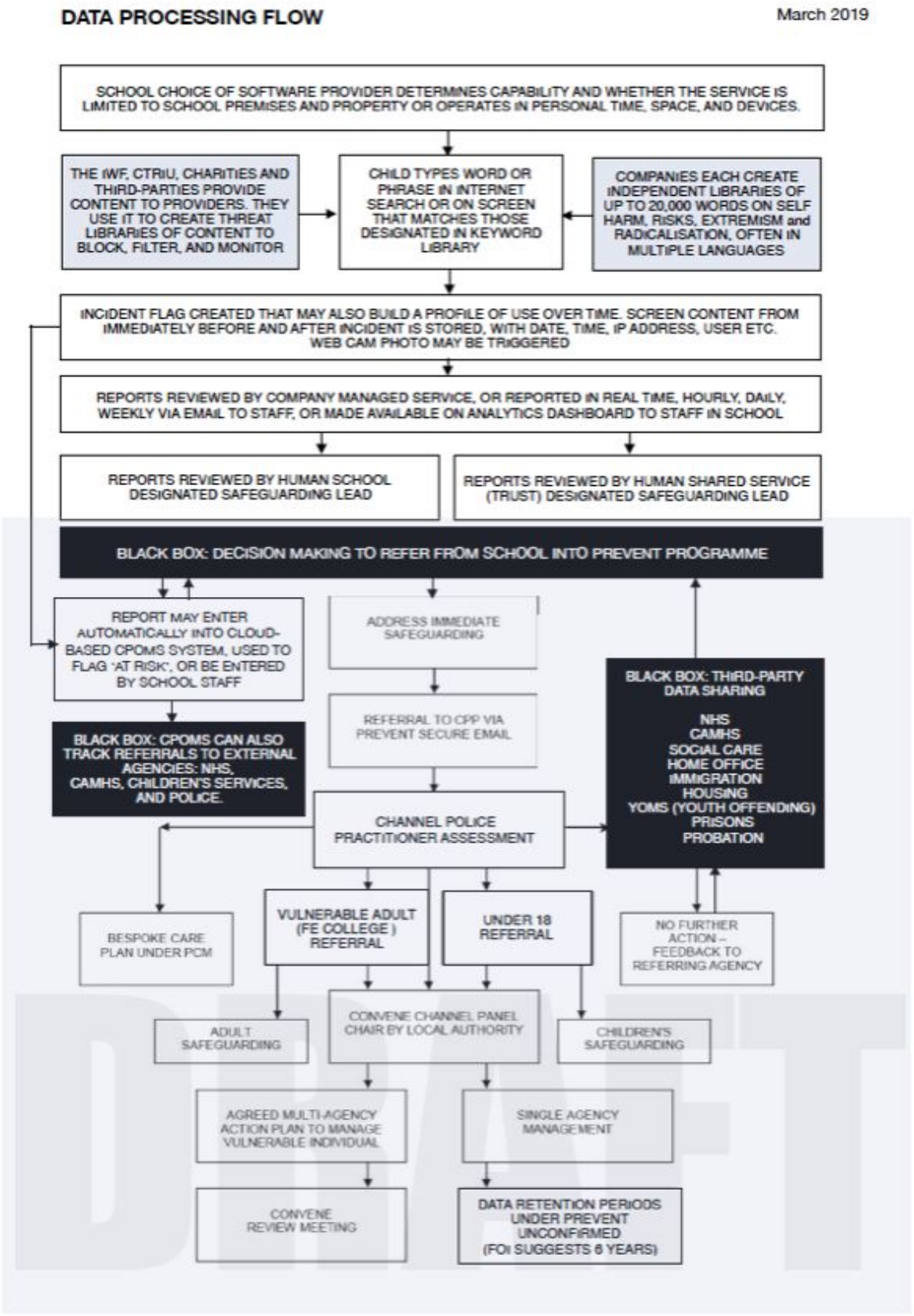
Children want to understand how their data are processed and restore fairness in systems, and power imbalances, as outlined for example in, *The Internet on our own Terms: how children and young people deliberated about their digital rights* (Jan 2017) (Research by Coleman, S., Pothong, K., Vallejos Perez, E., and Koene, A. supported by 5Rights, Horizon, Universities of Leeds and of Nottingham). The bodies with whom they interact should therefore be accountable to them, their families, the wider public and civil society.

The direction of travel (throughout the process as referrals leave a school setting and until a child's completion through the process, shaded in our diagram) is for information to become harder to access, and ever more limited, with the result that such bodies are becoming ever less accountable at the same time as more processing is done by third parties, at home and abroad.

Since over 70% of referrals result in no further processing, and over a third of referrals come from the education sector in England, we believe significantly more accountability is required in this area of public sector activity. With all the caveats of properly applied exemptions for personal data protection and policy,we recommend a duty of transparency and accountability should apply to these bodies.

[20] State of Data survey carried out 17-20 February 2018 https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

B. Diagram: Children's data flows processed into, across and out of Prevent



II. Civil Liberties groups' shared concerns

1. A chronic lack of transparency

Rights Watch (UK) and Liberty are concerned that, despite broad policy statements of compliance with data protection and privacy rights, the operation of the Prevent strategy and the Channel programme on the ground does not demonstrate due respect for transparency, or personal information and privacy.

"*From the case studies considered by RW(UK) in its 2016 report, 'Preventing Education?*[21] *it appears local authorities, schools, and police authorities may be operating some system of data collection and sharing which records a child's interaction with the Prevent strategy or the Channel programme. This could include formal referrals, informal information and events such as a police visit to a child's home. RW(UK) and Liberty have significant concerns about the rigour and compliance of such a system of data collection with both the specific requirements of data protection laws and the Human Rights Act".*

CRIN (Child Rights International Network) told us,
"*The Channel programme operates through panels, led by a representative of the police (the Channel Police Practitioner) and can include professionals from education, social work, immigration, housing and health services. Each panel is formed at the discretion of individual local authorities, and so their size and make up vary significantly across the country ...**there is a chronic lack of transparency about the way that information is collected and fed into this process, including within schools."***

CRIN used freedom of information requests in an attempt to find out the ways that schools are using [Internet] filtering and monitoring programs to detect signs of "radicalisation" in students.

"*CRIN submitted 61 requests to schools across a London Borough to ask what filtering and monitoring programs were installed on school ICT equipment for the purposes of detecting signs of "radicalisation", information about how the software worked and how many students had been flagged up by the software [in 2016].* ***None of the schools provided detailed information and a common response was that their filtering software was operated by a public-private agreement that is not subject to the Freedom of Information Act."***

"***without a clear picture of what information schools, or private companies working on behalf of schools, are collecting and where it is held, it is impossible to assess the adequacy of mechanisms to protect the data of children. The outsourcing of services to the private sector has also has extended the number of bodies involved.*****"**

2. Impact on equality and human rights

FOI is one of the only tools open to all, to defend human rights. As ever more public sector work is outsourced to the powerful but opaque private sector, the checks and balances required to uphold equality and human rights, fail in their reach, and limit the ability of civil society to perform this task. We often need facts to support individuals to seek redress when rights and freedoms are infringed upon, or to scrutinise and challenge policy and practice which does not uphold ethical and lawful practice and the reasonable expectations of society. Freedom of Information must also be easily enforceable on behalf of children by others, to champion their rights. Ever more legislation is made with ever less scrutiny, and the direction of travel is to embed this. FOI needs strengthened to uphold children's rights across their everyday interactions with the State and companies, fit for today's state infrastructure.[22]

[21] Rights Watch UK report, *'Preventing Education?'* (2016)
https://defenddigitalme.com/wp-content/uploads/2019/02/preventing-education-final-to-print-3.compressed-1.pdf.
[22] Who'll uphold children's rights as we leave the EU? Jen Persson in Open Democracy, February 2019
https://www.opendemocracy.net/en/opendemocracyuk/who-ll-protect-children-s-rights-as-we-leave-eu/

III. Recommendations

"It's difficult to know what or who to trust. Misinformation is spreading. Politics and the media are being pushed to the limit by advancements in technology and uncertainty about the future. We need facts more than ever." [Full Fact, 2019]

1. Expansion

1) With reference to recommendations in section 2.3.1 of the ICO report[23] we support the expansion of the remit of the FOIA 2000 to any body contracted to perform, or engaged in, provision of public sector activity, funded in any part by public funds, or powers inferred from statutory duties.
2) This expansion should explicitly include Exam Boards, and Children's Safeguarding Boards / Multi Agency Safeguarding Hubs, as well as bodies involved in children's social care.
3) Encourage proactive disclosure of information, including open data opportunities by Exam Boards, and Children's Safeguarding Boards / Multi Agency Safeguarding Hubs, children's social care and by commercial bodies in receipt of public funding, or performing activities as an outsourced arm of the public sector, while making a duty of minimum transparency not a voluntary, but enforceable action.
4) Obligations of transparency should be mindful of the people involved in the activity affected by the public body and its work outsourced to the private sector, and give extra weight to an obligation on the body where the individuals are particularly vulnerable, including the disabled and children.

2. Enforcement

1) Consistent enforcement of non-compliance with timely responses by public bodies under the Freedom of Information Act 2000.
2) A mechanism of urgent redress for organisations with duties similar to those set out in Article 80 of the General Data Protection Regulation, could be used to draw such cases to the attention of the regulator before the case reaches its full conclusion. While time periods are set under the FOIA 2000, reality is that the completion of the Internal Review process, rather than the statutory time period, is seen as the trigger for ICO enforcement. This is currently inadequate. A new mechanism would be helpful to encourage timely compliance without first having to complete the full appeal process with the public body, which is the very same public body dragging its heels to respond and hindering the FOI process.

3. Education

1) We suggest that the public understanding of the Freedom of information process should include explanations of rights to the complete process, including the role of the Information Rights First Tier Tribunal, and what support is available so that the process is not seen as a barrier to pursuit.
2) Education should be part of a wider package of explanation of personal data and information rights.

About defenddigitalme and what we do

We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England and beyond. We are funded 2017-19 through an annual grant from the Joseph Rowntree Reform Trust Ltd. We are happy to answer any questions, or support further work and research with civil society, as part of this consultation.

Contact: info@defenddigitalme.com

[23] Outsourcing Oversight? The case for reforming access to information law p22 https://ico.org.uk/media/2614204/outsourcing-oversight-ico-report-to-parliament.pdf