Defend Digital Me

April, 2025

Our recommendation to delay children's personal data distribution under the Wales Pilot

I am writing on behalf of Defend Digital Me, to express our concerns about your pupils and/or patients potential involvement in the Welsh Government data extraction project with pilot authorities:

Cardiff County Council
Carmarthenshire County Council
Gwynedd County Council
Isle of Anglesey County Council
Monmouthshire County Council
Powys County Council
Rhondda, Cynon, Taff County Borough Council

We urge you to

(a) not proceed with data transfers until questions and clarifications have been addressed and all of your data protection obligations and those of others in this process are met,

(b) seek and follow your own data protection and legal advice.

And we would welcome your engagement with us, to help understand the current situation while we advocate for safe, fair transparent data practices that protects the best interests of the child, and all learners in educational settings.

It is not clear that any involved school setting, health setting, or the Welsh Government meets the necessary conditions and obligations in data protection law that would follow in practice from these legislative changes. We would welcome your engagement to ensure our understanding is accurate, and that we can engage in an informed and constructive way with

stakeholders, such as the WG authorities, Westminster policy makers and the DfE, The Information Commissioner's Office and schools and health settings.

Request for engagement and information

If you are willing to help us better understand plans and to intervene, we would like to ask you for some information about the pilot in your setting. We will also do our best to support any questions you may have, and we are non-partisan, and have no religious or other affiliation.

Basic practicalities

1. Has the Welsh Government or Council informed you about these proposals, and when? Did these include discussion of how to do it, such as an offer of any alternatives that do not require data copying and transfer? For example better privacy-preserving methods of cross-referencing your children exist, rather than sending data around systems which is generally seen as an outdated method, and creates higher data processing risks than enabling secure access to the data.
2. Have you gone ahead already, what dates do you intend to start and finish the data transfers, or have you decided to wait before proceeding and put it on pause?
3. Please confirm the total number of pupils/patients on register in scope, as of April 30th, 2025.

Data Protection matters of law

4. For schools only, have you consulted parents and pupils on the linkage of school records with health data, and the parties in (6)? (informed fair processing obligations)
5. For health settings only, have you consulted patients on the health data transfer to Local Authorities and linkage with education records? (informed fair processing obligations)
6. As of April 29th 2025, we understand that the records have been extracted from a single source, the NHS Shared Service Partnerships, described in the DPIA as a data processor. Was this under your instruction, and have you been informed of it?

Please can you also provide a copy (if you have one) of:

7. The data protection impact assessment (DPIA) undertaken by the school for this pilot or any undertaken by another third party eg the Welsh Government, including an identified lawful basis for Article 6 and a separate condition for processing under Article 9 as set out in Schedule 1 of the DPA 2018.
8. A copy of the information you or others have given to the children or families about the processing of their information in your care, as set out on page 2 above.

We set out our understanding of the cumulative legislative changes in Wales and Westminster, the concerns we have and their basis in law and background below. Not least that **security of the data infrastructure appears unfit for purpose** as the BBC recently reported[1] the personal details of vulnerable children in Cardiff had been compromised due to a data breach, evidenced in council documents. The cybersecurity failure poses "**a potential safeguarding risk to children**" and relates to young people looked after by Cardiff council, according to the Local Democracy Reporting Service. "*The failure affected Data Cymru, which is a Welsh local government company with a board of directors elected by the Welsh Local Government Association (WLGA)* ***that supports councils and their partners to collect data***".

Thank you for your consideration. We look forward to receiving your response, if you were able, as soon as possible given the hurried nature of the proposals and legislative window for the data transfers process.

I am happy to answer any questions you may have, or to discuss by email or telephone/video call on request as well, or if you prefer it over email, my contact details as below.

Sincerely,

Jen Persson
Director, Defend Digital Me
jen@defenddigitalme.org

Defend Digital Me 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. | https://defenddigitalme.org/

[1] Vulnerable children's details at risk in data breach (BBC) March 27, 2025 https://www.bbc.co.uk/news/articles/cp8l6xx6r84o

Summary of legislative changes underway

A. The Children Act 2004 (Children Missing Education Database) (Pilot) (Wales) Regulations 2025[2] come into force on 8 April 2025 and cease to have effect on 8 April 2026. It requires a **Local Health Board, or a GMS contractor**[3], that holds any of the information specified in relation to any child who is "usually resident" in a pilot local authority's area to disclose it to the child's relevant pilot Local Authority by 30 April 2025.

1. The child's name (including any former name).
2. The child's address (or last known address) including postcode.
3. The child's date of birth.

These data from the **Local Health Board, or a GMS contractor will be added together with these further information in the "CME data" that Local Authorities creates from linkage**

4. Name, address, postcode, telephone number and email address of all parents of the child.
5. The name and address of the person providing all or part of the education.
6. **Any additional learning needs** that the child may have and any additional learning provision that is called for. [Our emphasis N.B. special category health data e.g. disabilities, hearing and sight impairments, mental or physical needs related to other conditions.]

B. The Education (Information about Children in Independent Schools) (Pilot) (Wales) Regulations 2025.[4] This affects every child in independent schools in seven Local Authorities in Wales, with effect from 8 April to 20 May 2025.

Information to be provided to the relevant local authority from the independent school is:

1. The child's name (including any former name).
2. The child's address (or last known address) including postcode.
3. The child's date of birth.

---

[2] The Children Act 2004 (Children Missing Education Database) (Pilot) (Wales) Regulations 2025 come into force on 8 April 2025 and cease to have effect on 8 April 2026 https://senedd.wales/media/tmqmngjx/sub-ld17052-e.pdf

[3] "The 2006 Act" ("Deddf 2006") means the National Health Service (Wales) Act 2006(1); "GMS contract" ("contract GMC") means a general medical services contract under section 42 of the 2006 Act (general medical services contracts: introductory); "GMS contractor" ("contractor GMC") means a party to a GMS contract, other than the Local Health Board; "usually resident" ("preswylio fel arfer") has the same meaning as in regulation 2(2) and (3) of the Local Health Boards (Directed functions) (Wales) Regulations 2009(2) https://senedd.wales/media/tmqmngjx/sub-ld17052-e.pdf

[4] https://www.legislation.gov.uk/wsi/2025/308/schedule/1/made

C**. The Children's Wellbeing and Schools Bill.** This affects every child in any educational setting, including Wales, with commencement once the Bill passes into law, expected in 2025. On March 17th, the government significantly expanded the Bill that had been only about England, to now include Wales, only after all the stages of scrutiny in the House of Commons were over. The new law amends both *the Education Act 1996* and *The Children Act 2004*, to compel state registration of learners under 19 and their providers of almost any type of education, who are ***outside*** state-funded settings. The changes affect every child in Wales—including those in private independent schools, as well as those in Elective Home Education (EHE) and otherwise not in state education, and includes powers to transfer data from Local Authorities (in Wales) to the Secretary of State (the Westminster Department for Education).

Summary concerns

1. With regard to Data Protection Law and questions of Human Rights

As you will know, children merit specific protection with regard to their personal data in UK data protection law, under the GDPR and under the Convention 108 as applied to the UK, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Children also merit specific considerations and legal protections in Wales, that follow on from the adoption of the UNCRC into domestic law.

1.1 Duties under UK Data Protection Law and obligations of the data controller

The Welsh Government Data Protection Impact Assessment[5] claims that it is not the data controller. We think this is incorrect. The Welsh Government has determined the need and the nature of processing, the purposes for which the data are processed, its timing, and the means of processing. These have been decided by the Welsh Government ("WG") and passed on to the Local Authorities and educational settings and health settings to exercise even down to the dates within which the pilot must be carried out.

In our view the WG *is* the data controller for these new sets of data processing and must

[5] The Draft Children Act 2004 Children Missing Education Database (Wales) Regulations 2025 Data Protection Impact Assessment (page 6) https://defenddigitalme.org/wp-content/uploads/2025/04/DPIA-2024-25-CME-database-1.pdf

therefore comply with all of the lawful obligations of a data controller.[6] It makes no difference the WG does not directly access the data. It does matter to schools and Local Health Boards who at best are joint controllers of the same data but not for the same purposes, and who have been subject to a direction not made the decision or able to control the details of the nature of the processing themselves.

We believe that educational settings and Local Health Boards and GPs, as well as data subjects, all need urgent clarity and definitive view from the ICO on this matter.

Who is the data controller is very significant in law, as:

> (a) it must be clearly expressed in a privacy notice to the data subjects as part of fair processing, with a named party responsible for the data processing.
>
> (b) It must be clear to all stakeholders who is accountable to the data subjects for ensuing their rights in law are met, for sending them the information to fulfil fair processing obligations in an accessible manner suitable for a child, for questions about the processing, or for example should data subjects wish to make complaints to the ICO, or pursue legal action.

1.2 Duties under UK Data Protection Law and the lawful basis

A data controller or processor, whether a school setting, health board or GP, must protect children's personal data, in accordance with the Data Protection Act 2018 ("DPA 2018"), the UK GDPR and Convention 108, and requires the identification of a lawful basis that must be communicated to the data subjects (the people the personal data involved, are about).

Health data, which is defined as "special category" or "sensitive" data under the UK GDPR and Convention 108, have additional requirements, subject to a high level of protection. In order to process health data, you must identify both a lawful basis under both Article 6 of the UK GDPR and a separate condition for processing under Article 9, some of which require additional conditions and safeguards under UK law, set out in Schedule 1 of the DPA 2018.[7]

Further, parties are required to comply with the principles of purpose limitation and security:

---

[6] ICO Guidance on data controllers https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors-a-guide/

[7] Special category data - ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

- Ensure that data are used only for the purposes for which they are obtained and that such data are not unlawfully disclosed to third parties. If a purpose is identified, it could only be considered a lawful purpose under the DPA if no less intrusive methods could be used to achieve the same aim.
- Store data securely to prevent any unauthorised or unlawful use.

The lawful basis under data protection law is unclear for the processing of health data from Local Health Boards and from independent school settings to Local Authorities. If the original lawful basis for processing personal data was consent, one cannot simply assume another basis for any new processing activity. Consent is often invalid for the education sector given the power imbalance between the child/family and school authority and therefore rarely the basis for data processing, instead relying on contract (independent schools) or public task (state schools). But the lawful basis for data processing for the same data cannot simply be switched to another, without legal assessment and fair processing.

1.3 Duties of Informed processing under UK Data Protection Law

The principle of fair processing: Notification sent to data subjects ("the children") and their parents must include information about the processing of their child's personal data that is sufficient to ensure that parents are fully informed about what is being proposed.
The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used, in particular where the data subject is a child.
This should include details about the named data controller, the type of information to be taken, how it will be used, the parents' and the pupil's full range of rights including the right to object under the lawful basis used of public task, and the school's duty to provide explanation of the rights of the child in language that is understandable to a child.
Under Article 8 of Convention 108[8] Certain essential information has to be compulsorily provided in a proactive manner by the controller to the data subjects when directly or indirectly (not through the data subject but through a third-party) collecting their data, subject to the possibility to provide for exceptions in line with Article 11 paragraph 1. Information on the name and address of the controller (or co-controllers), the legal basis and the purposes of the data processing, the categories of data processed and recipients, as well

[8] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

as the means of exercising the rights can be provided in any appropriate format (either through a website, technological tools on personal devices, etc.) as long as the information is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (for example, in a local or in a child friendly language where necessary.

1.4 Court decisions in support of fair processing obligations

Court decisions support the necessity for fully informed processing. For example, the case CJEU - C-201/14 - Bara and Others (2015)[9] held transferring personal data between public administrative bodies requires informing the concerned data subjects of transfer and processing.

> *"Article 315 (currently 322) of Romanian Law No 95/2006 mandated that all public authorities must transmit any data necessary to determine the insurance status of individuals to the National Health Insurance Fund (CNAS).*
>
> *"The Court and the Advocate General agreed that the principle of fair processing "requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient". Without the transparency of such information, the exercise of other rights (e.g., to rectify, to object) would not be possible. This principle was later cited by the Belgian data protection authority in APD/ GBA – 47/2022.*
>
> *"Lastly, Article 11 Directive 95/46 concerns the information required to be communicated if the data was not collected directly from the data subject. The Court considered that, after the data transfer took place, the CNAS was under an obligation to provide information to the subjects concerning the purpose of the processing and the categories of data concerned. Article 11(2) also provides Member States with the possibility of setting aside the obligation of information through a legislative measure. The Court reiterated that the 2007 Protocol did not meet this requirement. The Court concluded that Articles 10, 11, and 13 Directive 95/46 preclude national measures from allowing a public administrative body to transfer personal data to another public authority without informing the data subjects concerned of the transfer and the subsequent processing."*

2. Human Rights grounds: The UN Convention on the Rights of the Child (UNCRC) and ECHR

This processing raises **significant privacy concerns, rights that are protected by law**. Given the unnecessary and disproportionate interference there is further likely a breach of the Convention 108 and Data Protection Act 2018. Disclosure of a person's personal data *prima*

[9] https://gdprhub.eu/index.php?title=CJEU_-_C-201/14_-_Bara_and_Others

facie engages rights under Article 8.1 and 8.2 of the European Convention on Human Rights. Disproportionate data transfers are likely in violation of the Human Rights Act 1998, where the law states that a privacy invasion must be proportionate to the threat.

Wales has directly incorporated the United Nations Convention on the Rights of the Child (UNCRC) into domestic law under the Rights of Children and Young Persons (Wales) Measure 2011 - underlining Wales' commitment to children's rights and the UNCRC.

Under the UNCRC Article 16: "No child shall be subjected to arbitrary or unlawful interference with his or her privacy." As per Article 16(2), *"The child has the right to the protection of the law against such interference."* As such, without informing the children, in addition to the violation of data protection laws, it is highly likely that schools doing so are acting in breach of UNCRC Article 16 and Article 12, "*the right to be heard*" and have their views taken into account in matters of significance.

Furthermore the data sharing creates **risks of discrimination and breach of the public sector equality duty** since the *Children's Wellbeing and Schools Bill equalities impact assessment*,[10] for which this Wales project is in effect, not only a Welsh but a UK national policy pilot, "*we recognise that the [Children Not in School] CNIS proposals may have a disproportionate impact on those of Jewish ethnicity and the Gypsy, Roma, Traveller (GRT) community*."

3. Sharing information is subject to a number of other legal constraints outside data protection law. The regulation is a wholly unsuitable legislative vehicle for such significant change of national policy. To mandate data transfers from medical bodies, mandates a **breach of the common law obligations of doctor-patient confidence** and while confidentiality is not an absolute bar to disclosure, one must make a judgement as to where the public interest lies (the more sensitive and damaging the information, the stronger the public interest in disclosure will need to be). The data required includes health data as set out as above (**Any additional learning needs** that the child may have and any additional learning provision that is called for. [Our emphasis N.B. special category health data e.g. disabilities, hearing and sight impairments, mental or physical needs related to other conditions.]), not only name and contact details given in the health context. All of the children's personal data in question was communicated in circumstances giving rise to an obligation of confidence. Whether the obligation of confidence was express or implied from the circumstances given the special

[10] The Children's Wellbeing and Schools Bill equalities impact assessment (para 166, page 42) https://assets.publishing.service.gov.uk/media/67dd332070323a45fe6a6f19/CWS_Bill_Equalities_Impact_Assessment_as_amended_in__the_House__of_Commons.pdf

relationship between doctors and patients or schools and pupils, this obligation is enhanced, where there is risk of detriment to the subject.

4. The potential harms from the proposals to which this data transfers contribute have already been recognised by the Welsh Minister for Education, as laid out in the 2024 WG Child Rights Impact Assessment[11] of the broad measures, "**the proposals may result in a child not receiving their UNCRC article 24 right [to health], if families fail to register their children with health practitioners if didn't want their personal data shared**," and that, "**the proposals may challenge article 16 [Every child has the right to privacy.** The law should protect the child's private, family and home life], if child didn't want their personal data shared with the local authority by the health board."

5. No child on roll on a school register is a child missing education ("CME") but their data is being demanded in order to identify *others* who are. What alternatives for the identification of others were considered that would not involved processing *your* children's personal data at named child-level? Have measures been suggested that enable matching in privacy preserving ways? We believe the high bar of "*necessary* in a democratic society" is not met to allow the confidentiality breach of the vast majority of children by processing their personal data in order to identify a tiny minority. It is thus likely disproportionate and therefore unlawful under the UK GDPR for identifiable, sensitive data from children in your care to be copied and transferred for this purpose when more privacy preserving alternatives exist.

6. Purpose limitation does not extend to purposes that are not about the child in your care. The use of children's data by a Local Authority in order to identify *other* people's children, goes beyond the purposes for which your school collected it and explained it to the child and/or parents at the time of collection. Article 5(1)(b) states that personal data shall be:

> *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1),* ***not be considered to be incompatible with the initial purposes.****"*

[11] Children's rights impact assessment (draft): The Children Act 2004 Children Missing Education Database (Wales) Regulations 2025 https://www.gov.wales/childrens-rights-impact-assessment-draft-children-act-2004-children-missing-education-database

Would families and children who are in education, *reasonably expec*t that their personal data from educational and health settings is sent to the state on a coercive basis, in order to identify, support or punish other people's children who are not in receipt of education?

7. Furthermore, since the personal **data once received by Local Authorities, may then be transferred to the Westminster Department of Education**, which is likely to be made statutory under the forthcoming *Children's Wellbeing and Schools Bill* Clause 31, 436F, there are further serious privacy risks to children which have not been explained to them. The users and reuses via the Department for Education and their third party recipients, include commercial purposes. Access to identifying, pupil-level data since 2012[12] has included journalists[13], think tanks, charities, researchers and a wide range of others.[14] The Department has further aspirations to enable pupil data use for AI product development.[15] There are no safeguards in place to prevent any of these third party, including this commercial exploitation, of children in Wales as well, once the *Children's Wellbeing and Schools Bill* passes. A significant data breach, and an ICO Audit in 2020[16], identified a wide range of substantial concerns with the DfE national data processing procedures, including failure of fair processing and in commercial department practices, that have not yet been resolved.

8. Finally, we suggest that **security of the infrastructure appears unfit for purpose**. On March 27th, 2025, the BBC reported[17] the personal details of vulnerable children in Cardiff had been compromised due to a data breach, evidenced in council documents. The cybersecurity failure poses "**a potential safeguarding risk to children**" and relates to young people looked after by Cardiff council, according to the Local Democracy Reporting Service. "*The failure affected Data Cymru, which is a Welsh local government company with a board of directors elected by the Welsh Local Government Association (WLGA) **that supports councils and their partners to collect data***".

---

[12] Department for Education (DfE) approved data shares of identifying, often sensitive pupil-level data with external, third-party organisations since 2012 https://www.gov.uk/government/publications/dfe-external-data-shares

[13] Case study: press access sensitive pupil data https://www.whatdotheyknow.com/request/pupil_data_licensing_agreements_2/response/1088006/attach/22/l%20DR160915.02%20Application%20form%20Redacted.pdf

[14] https://www.whatdotheyknow.com/request/pupil_data_licensing_agreements_2#incoming-1079063

[15] Schools Week (2023) Minister wants schools to benefit from AI revolution https://schoolsweek.co.uk/minister-wants-schools-to-benefit-from-ai-revolution/

[16] Defenddigitalme timeline https://defenddigitalme.org/national-pupil-data-the-ico-audit-and-our-work-for-change-a-timeline/

[17] Vulnerable children's details at risk in data breach (BBC) March 27, 2025 https://www.bbc.co.uk/news/articles/cp8l6xx6r84o