**Safeguarding school-aged children from**

**neglect, harm, abuse, exploitation or violence through effective data sharing.**

All professional clinical staff and care staff understand their safeguarding responsibility to share data on vulnerable children with partners in the wider public service system as per

[The DfE data sharing advice to practitioners to safeguard children, 2018](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062969/Information_sharing_advice_practitioners_safeguarding_services.pdf) .

The full range of health care staff who care for school-aged children, including school nursing services, need to be particularly aware of this guidance due to the demonstrable increased vulnerability of school-aged children to safeguarding moments. We must all make every contact count when considering whether to share data whenever it is necessary to protect a child from significant harm.

Patient confidentiality is an important aspect of maintaining trust between clinicians and patients and no clinician wants to leave themselves open to an accusation of having potentially breached confidentiality by disclosing information that is not acted upon. All practitioners need to feel confident and willing to share the intelligence they have gathered about a child or a family - in order to help the school nurses, GPs and other staff to establish whether the information they hold is a key part of the jigsaw and there is a clear public interest in disclosing it to protect a child from harm.

The healthcare system has implemented the Child Protection Information System (CPIS) for those most vulnerable children on a child protection plan (including a few unborn children) and/ or a looked after child plan through the Local Authority Director of Childrens Services. It is therefore critical all clinical staff prioritise sharing data on these children.

[The Working Together Reforms August 2018](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2) gave us a statutory requirement to share across our partnership of healthcare, social services, and policing.

[Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents), sets out six key data protection principles which apply to safeguarding or law enforcement data processing by a competent authority i.e.:

* processing must be lawful and fair;
* the purposes of processing must be specified, explicit and legitimate;
* personal data must be adequate, relevant and not excessive;
* personal data must be accurate and kept up to date;
* personal data must be kept no longer than is necessary; and
* personal data must be processed in a secure manner.

NHS and health staff will always seek patient's consent to share their personal clinical data. However, staff are also aware that there are times when it is essential to share personal information to safeguard individuals or others from harm, and where it is appropriate to do so without patient consent. This is described as the **‘public interest’** argument in favour of disclosure. If consent cannot be obtained or isn’t operationally appropriate, you must provide a legitimate reason in your disclosure request proforma and describe the public interest in favour of disclosure in order to receive the requested data.

To avoid delays in receiving personal data for safeguarding purposes please ensure the data request meets the following:

* Always use appropriate official disclosure request proforma sanctioned by your organisation.
* Always send request through secure protectively marked email.
* Always provide clarification on whether or not consent has been sought.
* If consent is not obtained, a legitimate reason or ‘form of words’ must be provided to legally justify access patient/service user/staff member’s personal or sensitive information.
* Ensure that permissible powers and legal exemptions are being relied upon to share or process personal data.
* Always clearly explain in writing what specific/relevant information is required from the patient/service user/staff member record to assist with the case management of the individual in question. If the request is not specific – NHS staff will ask for further clarity

Practitioners may also seek consent and then, if the patient declines as is their right, then the practitioner might discuss with a senior colleague whether you use your professional duty of care and clinical prerogative to decide to share limited amount of data securely with another part of the safeguarding system which might protect the child from neglect, harm, abuse, exploitation, violence or death.

In summary, there is no UK law which states clinical teams caring for school-aged children cannot securely and lawfully share data between themselves.

We can, we will, we must share data if that information prevents safeguarding moments in any child’s life.



**Other reading ~**

[Confidentiality: good practice in handling patient information - ethical guidance - GMC (gmc-uk.org)](https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality)

Section 251 <https://digital.nhs.uk/services/data-access-request-service-dars/how-the-national-data-opt-out-affects-data-released-by-nhs-digital/national-data-opt-out-guidance-for-researchers/4-section-251-and-the-application-of-national-data-opt-outs>

**NHS Act 2006 Section 251 data sharing exemption** if a clinician thinks someone’s welfare is at risk or life is in danger.

**GDPR**

**Article 5**

1. Processing data shall be:
2. Processed lawfully, fairly and in a transparent manner in relation to the data subject

**Article 6**

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
2. The data subject has given consent to the processing of his or her personal data for one or more specific purposes…

(f)  processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Although, Article 6(1)(f) does not apply to processing carried out by public authorities in the performance of their tasks, in sharing information with DBS the data controller would not fall foul of this caveat as the information is shared for the DBS function rather than that of the Trust – ie for direct care purpose and any disclosure to protect the vital interests of individuals.

**Article 9**

Art 9 of GDPR sets out that processing of special categories of personal data is prohibited but this prohibition does not apply if, inter alia, the processing is necessary for reasons of substantial public interest (Art 9(2)(g). The GDPR principle of processing under “substantial public interest” is supplemented by provisions within the DPA 2018 as follows:

**Data Protection Act 2018.**

S10 (1)(b) makes provision about processing personal data set out in Art 9 (1) in reliance on one of the exceptions set out in Art 9(2). Art 9(2)(g) covers processing under substantial public interest.

S10(3) sets out that processing meets the requirement in point (g) of Art 9(2) for a basis in the law of the UK or part of the UK only if it meets a condition in Part 2 of Sch 1 to the DPA 2018.