In the opening chapter of "The Glass Consumer" (edited by Susan Lace, 2005), Perri 6 wrote "At least for the last 30 years or so, and perhaps for longer, we have lived in a personal information economy". Later in the chapter, there is clear evidence that use of collected personal information, before the digital economy, was shaping lives and limiting life chances for the disadvantaged. The mass collection of personal data has been in place for decades, but the 'gold rush' or 'arms race' that has accompanied the development of digital technologies, and particularly the rise of immersive technologies and persuasive design, have simply amplified this trend. This leads both to short-term and longer-term risks, but it is the latter that is so hard to comprehend, given the increased use of artificial intelligence and algorithms with unknown biases to process this vast amount of data. Further, machine learning adds a further black box to data processing, and few if any can 'understand' how machines come to the conclusions they do. The most disadvantaged may be subject to these algorithms, as for reasons of efficiency and cost-effectiveness, they become part of our public services and algorithmic biases may reinforce inequalities (see Eubanks, V: "Automating Inequality"). Whilst it is entirely possible to make some progress in helping young people understand the short-term risks of misuse of personal data (sharing passwords; geo-location risks; data breaches and hacked accounts) or use data visualisation to help them understand better its use, it is unlikely that they, or any living adult can predict how the masses of data currently collected will shape their futures. (Famously, Justin Mitchell, a Facebook Engineer commented "Probably 10 people in the world intimately understand the privacy calculations involved when you attempt to view a photo on Facebook." in 2010, giving some idea of the complexity of the challenge: http://www.quora.com/How-does-Facebook-Photos-privacy-work/answer/Justin-Mitchell). There is a further challenge when discussing risks with young people. Adolescents are, biologically, at their peak of health, and in addition to any impairment of judgement that occurs during the refashioning of the brain's judgement centres (frontal lobes) during puberty, anticipating future health or other risks is limited because they feel so alive and healthy. Perhaps this is rightly so, as they engage with, experiment and explore a world that they will soon inhabit as adults. But these combined factors make the notion of consent, even if sensitively obtained, barely fit for purpose when anticipating longer term impact in the use of personal data in a future rich with AI and machine learning. In health, sensitivities as top how personal health data could adversely affect a person's life's course led to the establishment of the Caldicott Guidelines, which though familiar are listed here for clarity: 1. Justify the purpose(s) Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian. 2. Don't use patient identifiable information unless it is necessary Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s). 3. Use the minimum necessary patient-identifiable information Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out. 4. Access to patient identifiable information should be on a strict need-to-know basis Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes. 5. Everyone with access to patient identifiable information should be aware of their responsibilities Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality. 6. Understand and comply with the law Every use of patient identifiable information must be lawful. Someone in each organisation handling patient

information should be responsible for ensuring that the organisation complies with legal requirements. 7. The duty to share information can be as important as the duty to protect patient confidentiality Professionals should in the patient's interest share information within this framework. Official policies should support them doing so. Whilst GDPR contains provisions intended to enhance the protection of children's personal data, and allow for a greater process of informed consent (rather than dark pattern design that forces agreement without choice), the Caldicott model could inform further how an ISS might be expected to act in relation to children. Further, as in health, even with young people's data being a special category under GDPR, there may be further sub-categories that are deemed even more sensitive, including health data. The spirit is one of aspiring to maximal data minimisation, and In that sense the following areas of concern could be addressed: 1. Reduction of the strategies used to encourage extended user engagement (persuasive design, as outlined by the 5Rights Foundation) would inevitably reduce the collection of online data. 2. Data minimisation (the collection of data that is only essential for service) should be the standard, and any purpose for use explicitly described. 3. Privacy settings are by default set to high, and maintained as such until a user actively decides, and has the competence to change them; less personal data is then shared. 4. Whilst profiling of young people's data under GDPR is given special attention in terms of impact, any resulting profiles might usefully be subject to strict retention and deletion processes, and be a special category for the right to erasure and rectification. All other categories for consideration are of value, and some, such as geo-location data, may be of sufficient risk to warrant early attention. However, the principle of obtaining and using the minimum data necessary is likely to build trust and positive use and should be the underpinning principle of age-appropriate design. Attached is a clear review of research and thinking about young people's capacity to consent in health services, and legal concepts such as competence and mental capacity could also inform the thinking.